

# Wireless Client and Wireless Access Point Manual

Document revision 2.3 (January 22, 2008, 8:53 GMT)

This document applies to V3.0

## Table of Contents

[Table of Contents](#)

[General Information](#)

[Summary](#)

[Quick Setup Guide](#)

[Specifications](#)

[Description](#)

[Wireless Interface Configuration](#)

[Description](#)

[Property Description](#)

[Notes](#)

[Example](#)

[Interface Monitor](#)

[Description](#)

[Property Description](#)

[Notes](#)

[Nstreme Settings](#)

[Description](#)

[Property Description](#)

[Notes](#)

[Example](#)

[Nstreme2 Group Settings](#)

[Description](#)

[Property Description](#)

[Notes](#)

[Example](#)

[Registration Table](#)

[Description](#)

[Property Description](#)

[Example](#)

[Connect List](#)

[Description](#)

[Property Description](#)

[Access List](#)

[Description](#)

[Property Description](#)

[Notes](#)

[Example](#)

[Info](#)

[Description](#)

[Property Description](#)

[Notes](#)

[Example](#)

## [Virtual Access Point Interface](#)

[Description](#)

[Property Description](#)

[Notes](#)

## [WDS Interface Configuration](#)

[Description](#)

[Property Description](#)

[Notes](#)

[Example](#)

## [Align](#)

[Description](#)

[Property Description](#)

[Command Description](#)

[Notes](#)

[Example](#)

## [Align Monitor](#)

[Description](#)

[Property Description](#)

[Example](#)

## [Frequency Monitor](#)

[Description](#)

[Property Description](#)

[Example](#)

## [Manual Transmit Power Table](#)

[Description](#)

[Property Description](#)

[Example](#)

## [Network Scan](#)

[Description](#)

[Property Description](#)

[Example](#)

## [Security Profiles](#)

[Description](#)

[Property Description](#)

[Notes](#)

## [Sniffer](#)

[Description](#)

[Property Description](#)

## [Sniffer Sniff](#)

[Description](#)

[Property Description](#)

[Command Description](#)

## [Sniffer Packets](#)

[Description](#)

[Property Description](#)

[Example](#)

## [Snooper](#)

[Description](#)

[Property Description](#)  
[Command Description](#)  
[Example](#)

## General Information

### Summary

This manual discusses management of Atheros and Prism chipset based wireless NICs that comply with IEEE 802.11 set of standards. These interfaces use radio waves as a physical signal carrier and are capable of data transmission with speeds up to 108 Mbps (in 5GHz turbo-mode).

MikroTik RouterOS supports the Intersil Prism II PC/PCI, Atheros AR5000, AR5001X, AR5001X+, AR5002X+, AR5004X+ and AR5006 chipset based cards for working as wireless clients (**station** mode), wireless bridges (**bridge** mode), wireless access points (**ap-bridge** mode), and for antenna positioning (**alignment-only** mode). For further information about supported wireless adapters, see [Device Driver List](#)

MikroTik RouterOS provides a complete support for IEEE 802.11a, 802.11b and 802.11g wireless networking standards. There are several additional features implemented for the wireless networking in RouterOS - WPA/WPA2 (Wi-Fi Protected Access), WEP (Wired Equivalent Privacy), software and hardware AES encryption, EAP authentication, WDS (Wireless Distribution System), DFS (Dynamic Frequency Selection), Alignment mode (for positioning antennas and monitoring wireless signal), VAP (Virtual Access Point), ability to disable packet forwarding among clients, Nstreme wireless transmission protocol and others. You can see the [table of features](#) supported by different cards.

The Nstreme protocol is MikroTik proprietary (i.e., incompatible with other vendors) 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 (Atheros AR5210 and newer MAC chips only) - one for transmitting data and one for receiving.

Benefits of Nstreme protocol:

- Client polling. Polling reduces media access times, because the card does not need to ensure the air is "free" each time it needs to transmit data (the polling mechanism takes care of it)
- Very low protocol overhead per frame allowing super-high data rates
- No implied protocol limits on link distance
- No implied protocol speed degradation for long link distances
- Dynamic protocol adjustment depending on traffic type and resource usage

### Quick Setup Guide

Let's consider that you have a wireless interface, called **wlan1**.

- To set it as an Access Point, working in 802.11g standard, using frequency **2442 MHz** and Service Set Identifier **test**, do the following configuration:

```
/interface wireless set wlan1 ssid=test frequency=2442 band=2.4ghz-b/g \  
mode=ap-bridge disabled=no
```

Now your router is ready to accept wireless clients.

- To make a point-to-point connection, using 802.11a standard, frequency **5805 MHz** and Service Set Identifier **p2p**, write:

```
/interface wireless set wlan1 ssid="p2p" frequency=5805 band=5ghz \  
mode=bridge disabled=no
```

The remote interface should be configured to station as showed below.

- To make the wireless interface as a wireless station, working in 802.11a standard and Service Set Identifier **p2p**:

```
/interface wireless set wlan1 ssid="p2p" band=5ghz mode=station disabled=no
```

## Specifications

Packages required: *wireless*

License required: *level4 (station and bridge mode), level5 (station, bridge and AP mode), levelfreq (more frequencies)*

Home menu level: */interface wireless*

Standards and Technologies: [IEEE802.11a](#), [IEEE802.11b](#), [IEEE802.11g](#)

Hardware usage: *Not significant*

## Description

The Atheros card has been tested for distances up to 20 km providing connection speed up to 17Mbit/s. With appropriate antennas and cabling the maximum distance should be as far as 50 km.

These values of **ack-timeout** were approximated from the tests done by us, as well as by some of our customers:

range	ack-timeout		
	5GHz	5GHz-turbo	2.4GHz-G
0km	default	default	default
5km	52	30	62
10km	85	48	96
15km	121	67	133
20km	160	89	174
25km	203	111	219
30km	249	137	368
35km	298	168	320
40km	350	190	375
45km	405	-	-

Please **note** that these are not the precise values. Depending on hardware used and many other factors they may vary up to +/- 15 microseconds.

You can also use **dynamic** ack-timeout value - the router will determine **ack-timeout** setting automatically by sending periodically packets with a different ack-timeout. Ack-timeout values by which ACK frame was received are saved and used later to determine the real ack-timeout.

The Nstreme protocol may be operated in three modes:

- **Point-to-Point mode** - controlled point-to-point mode with one radio on each side
- **Dual radio Point-to-Point mode (Nstreme2)** - the protocol will use two radios on both sides simultaneously (one for transmitting data and one for receiving), allowing superfast point-to-point connection
- **Point-to-Multipoint** - controlled point-to-multipoint mode with client polling (like AP-controlled TokenRing)

## Hardware Notes

The MikroTik RouterOS supports as many Atheros chipset based cards as many free adapter slots are on your system. One license is valid for all cards on your system. **Note** that maximal number of PCMCIA sockets is 8.

Some chipsets are not stable with Atheros cards and cause radio to stop working. MikroTik RouterBoard 200, RouterBoard 500 series, and systems based on Intel i815 and i845 chipsets are tested and work stable with Atheros cards. There might be many other chipsets that are working stable, but it has been reported that some older chipsets, and some systems based on AMD Duron CPU are not stable.

Only AR5212 and newer Atheros MAC chips are stable with RouterBOARD200 connected via RouterBOARD14 four-port MiniPCI-to-PCI adapter. This note applies only to the RouterBOARD200 platform with Atheros-based cards.

## Wireless Interface Configuration

Home menu level: */interface wireless*

### Description

In this section we will discuss the most important part of the configuration.

### Property Description

**ack-timeout** (*integer | dynamic | indoors*) - acknowledgement code timeout (transmission acceptance timeout) in microseconds for acknowledgement messages. Can be one of these:

- **dynamic** - ack-timeout is chosen automatically
- **indoors** - standard constant for indoor usage

**adaptive-noise-immunity** (yes | no; default: **yes**) - adjust various receiver parameters dynamically to minimize interference and noise effect on the signal quality. Only AR6001XL and AR6001GL and newer Atheros chips support this feature

**allow-sharedkey** (yes | no; default: **no**) - allow WEP Shared Key clients to connect. Note that no authentication is done for these clients (WEP Shared keys are not compared to anything) - they are just accepted at once (if access list allows that)

**antenna-gain** (*integer*; default: **0**) - antenna gain in dBi. This parameter will be used to calculate whether your system meets regulatory domain's requirements in your country

**antenna-mode** (*ant-a | ant-b | rxa-txb | txa-rxb*; default: **ant-a**) - which antenna to use for transmit/receive data:

- **ant-a** - use only antenna a
- **ant-b** - use only antenna b
- **rxa-txb** - use antenna a for receiving packets, use antenna b for transmitting packets
- **txa-rxb** - use antenna a for transmitting packets, antenna b for receiving packets

**area** (*text*; default: **""**) - string value that is used to describe an Access Point. Connect List on the Client's side comparing this string value with area-prefix string value makes decision whether allow a Client connect to the AP. If area-prefix match the entire area string or only the beginning of it the Client is allowed to connect to the AP

**arp** (*disabled | enabled | proxy-arp | reply-only*; default: **enabled**) - Address Resolution Protocol setting

**band** - operating band

- **2.4ghz-b** - IEEE 802.11b
- **2.4ghz-b/g** - IEEE 802.11g (supports also legacy IEEE 802.11b protocol)
- **2.4ghz-g-turbo** - IEEE 802.11g using double channel, providing air rate of up to 108 Mbit
- **2.4ghz-onlyg** - only IEEE 802.11g
- **5ghz** - IEEE 802.11a up to 54 Mbit
- **5ghz-turbo** - IEEE 802.11a using double channel, providing air rate of up to 108Mbit
- **2ghz-10mhz** - variation of IEEE 802.11g with half the band, and, accordingly, twice lower speed (air rate of up to 27Mbit)
- **2ghz-5mhz** - variation of IEEE 802.11g with quarter the band, and, accordingly, four times lower speed (air rate of up to 13.5Mbit)
- **5ghz-10mhz** - variation of IEEE 802.11a with half the band, and, accordingly, twice lower speed (air rate of up to 27Mbit)
- **5ghz-5mhz** - variation of IEEE 802.11a with quarter the band, and, accordingly, four times lower speed (air rate of up to 13.5Mbit)

**basic-rates-a/g** (*multiple choice: 6Mbps, 9Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps*; default: **6Mbps**) - basic rates in 802.11a or 802.11g standard. This should be the minimal speed all the wireless network nodes support (they will not be able to connect otherwise). It is recommended to leave this as default

**basic-rates-b** (*multiple choice: 1Mbps, 2Mbps, 5.5Mbps, 11Mbps*; default: **1Mbps**) - basic rates in 802.11b mode. This should be the minimal speed all the wireless network nodes support (they will not be able to connect otherwise). It is recommended to leave this as default

**burst-time** (*time*; default: **disabled**) - time in microseconds which will be used to send data without stopping. Note that no other wireless cards in that network will be able to transmit data during burst-time microseconds. This setting is available only for AR5000, AR5001X, and AR5001X+ chipset based cards

**compression** (*yes | no*; default: **no**) - if enabled on AP (in ap-bridge or bridge mode), it advertizes that it is capable to use hardware data compression. If a client, connected to this AP, also supports and is configured to use the hardware data compression, it requests the AP to use compression. This

property does not affect clients, which do not support compression.

**country** (*albania | algeria | argentina | armenia | australia | austria | azerbaijan | bahrain | belarus | belgium | belize | bolivia | brazil | brunei darussalam | bulgaria | canada | chile | china | colombia | costa rica | croatia | cyprus | czech republic | denmark | dominican republic | ecuador | egypt | el salvador | estonia | finland | france | france\_res | georgia | germany | greece | guatemala | honduras | hong kong | hungary | iceland | india | indonesia | iran | ireland | israel | italy | japan | japan1 | japan2 | japan3 | japan4 | japan5 | jordan | kazakhstan | korea republic | korea republic2 | kuwait | latvia | lebanon | liechtenstein | lithuania | luxemburg | macau | macedonia | malaysia | mexico | monaco | morocco | netherlands | new zealand | no\_country\_set | north korea | norway | oman | pakistan | panama | peru | philippines | poland | portugal | puerto rico | qatar | romania | russia | saudi arabia | singapore | slovak republic | slovenia | south africa | spain | sweden | switzerland | syria | taiwan | thailand | trinidad & tobago | tunisia | turkey | ukraine | united arab emirates | united kingdom | united states | uruguay | uzbekistan | venezuela | viet nam | yemen | zimbabwe*; default: **no\_country\_set**) - limits wireless settings (frequency and transmit power) to those which are allowed in the respective country

- **no\_country\_set** - no regulatory domain limitations

**default-ap-tx-limit** (*integer*; default: **0**) - limits data rate for each wireless client (in bps)

- **0** - no limits

**default-authentication** (*yes | no*; default: **yes**) - specifies the default action on the client's side for APs that are not in connect list or on the AP's side for clients that are not in access list

- **yes** - enables AP to register a client if it is not in access list. In turn for client it allows to associate with AP not listed in client's connect list

**default-client-tx-limit** (*integer*; default: **0**) - limits each client's transmit data rate (in bps). Works only if the client is also a MikroTik Router

- **0** - no limits

**default-forwarding** (*yes | no*; default: **yes**) - whether to use data forwarding by default or not. If set to 'no', the registered clients will not be able to communicate with each other

**dfs-mode** (*none | radar-detect | no-radar-detect*; default: **none**) - used for APs to dynamically select frequency at which this AP will operate

- **none** - do not use DFS
- **no-radar-detect** - AP scans channel list from "scan-list" and chooses the frequency which is with the lowest amount of other networks detected
- **radar-detect** - AP scans channel list from "scan-list" and chooses the frequency which is with the lowest amount of other networks detected, if no radar is detected in this channel for 60 seconds, the AP starts to operate at this channel, if radar is detected, the AP continues searching for the next available channel which is with the lowest amount of other networks detected

**disable-running-check** (*yes | no*; default: **no**) - disable running check. If value is set to 'no', the router determines whether the card is up and running - for AP one or more clients have to be registered to it, for station, it should be connected to an AP. This setting affects the records in the routing table in a way that there will be no route for the card that is not running (the same applies to dynamic routing protocols). If set to 'yes', the interface will always be shown as running

**disconnect-timeout** (*time*; default: **3s**) - time since the third sending failure ( 3\*(hw-retries+1) packets have been lost) at the lowest datarate only (i.e. since the first time on-fail-retry-time has been activated), when the client gets disconnected (logged as "extensive data loss")

**frame-lifetime** (*integer*; default: **0**) - frame lifetime in centiseconds since the first sending attempt

to send the frame. Wireless normally does not drop any packets at all until the client is disconnected. If there is no need to accumulate packets, you can set the time after which the packet will be discarded

- **0** - never drop packets until the client is disconnected (default value)

**frequency** (*integer*) - operating frequency of the AP (ignored for the client, which always scans through its scan list regardless of the value set in this field)

**frequency-mode** (*regulatory-domain | manual-tx-power | superchannel*; default: **regulatory-domain**) - defines which frequency channels to allow

- **regulatory-domain** - use the channels allowed in the selected country at the allowed transmit power (with the configured antenna-gain deducted) only. Also note that in this mode card will never be configured to higher power than allowed by the respective regulatory domain
- **manual-tx-power** - use the channels allowed in the selected country only, but take transmit power from the tx-power settings
- **superchannel** - only possible with the Superchannel license. In this mode all hardware supported channels and transmit power settings are allowed

**hide-ssid** (*yes | no*; default: **no**) - whether to hide ssid or not in the beacon frames:

- **yes** - ssid is not included in the beacon frames. AP replies only to probe-requests with the given ssid
- **no** - ssid is included in beacon frames. AP replies to probe-requests with the given ssid and to 'broadcast ssid' (empty ssid)

**hw-retries** (*integer*; default: **15**) - number of frame sending retries until the transmission is considered failed. Data rate is decreased upon failure, but if there is no lower rate, 3 sequential failures activate on-fail-retry-time transmission pause and the counter restarts. The frame is being retransmitted either until success or until client is disconnected

**interface-type** (*read-only: text*) - adapter type and model

**mac-address** (*MAC address*) - Media Access Control (MAC) address of the interface

**master-interface** (*name*) - physical wireless interface name that will be used by Virtual Access Point (VAP) interface

**max-station-count** (*integer: 1..2007*; default: **2007**) - maximal number of clients allowed to connect to AP. Real life experiments (from our customers) show that 100 clients can work with one AP, using traffic shaping

**mode** (*alignment-only | ap-bridge | bridge | nstreme-dual-slave | station | station-pseudobridge | station-pseudobridge-clone | station-wds | wds-slave*; default: **station**) - operating mode:

- **alignment-only** - this mode is used for positioning antennas (to get the best direction)
- **ap-bridge** - the interface is operating as an Access Point
- **bridge** - the interface is operating as a bridge. This mode acts like ap-bridge with the only difference being it allows only one client
- **nstreme-dual-slave** - the interface is used for nstreme-dual mode
- **station** - the interface is operating as a wireless station (client)
- **station-pseudobridge** - wireless station that can be put in bridge. MAC NAT is performed on all traffic sent over the wireless interface, so that it look like coming from the station's MAC address regardless of the actual sender (the standard does not allow station to send packets with different MAC address from its own). Reverse translation (when replies arrive from the AP to the pseudobridge station) is based on the ARP table. Non-IP protocols are being sent to the

default MAC address (the last MAC address, which the station has received a non-IP packet from). That means that if there is more than one client that uses non-IP protocols (for example, PPPoE) behind the station, none of them will be able to work correctly

- **station-pseudobridge-clone** - similar to the station-pseudobridge, but the station will clone MAC address of a particular device (set in the station-bridge-clone-mac property), i.e. it will change its own address to the one of a different device. In case no address is set in the station-bridge-clone-mac property, the station postpones connecting to an AP until some packet, with the source MAC address different from any of the router itself, needs to be transmitted over that interface. It then connects to an AP with the MAC address of the device that have sent that packet
- **station-wds** - the interface is working as a station, but can communicate with a WDS peer
- **wds-slave** - the interface is working as it would work in ap-bridge mode, but it adapts to its WDS peer's frequency if it is changed

**mtu** (*integer*; 68..1600; default: **1500**) - Maximum Transmission Unit

**name** (*name*; default: **wlanN**) - assigned interface name

**noise-floor-threshold** (*integer* | *default*: -128..127; default: **default**) - noise strength in dBm below which the card will transmit

**on-fail-retry-time** (*time*; default: **100ms**) - time, after which we repeat to communicate with a wireless device, if a data transmission has failed 3 times on the lowest rate

**periodic-calibration** (*default* | *disabled* | *enabled*; default: **default**) - to ensure performance of chipset over temperature and environmental changes, the software performs periodic calibration

**periodic-calibration-interval** (*integer*; default: **60**) - interval between periodic recalibrations, in seconds

**preamble-mode** (*both* | *long* | *short*; default: **both**) - sets the synchronization field in a wireless packet

- **long** - has a long synchronization field in a wireless packet (128 bits). Is compatible with 802.11 standard
- **short** - has a short synchronization field in a wireless packet (56 bits). Is not compatible with 802.11 standard. With short preamble mode it is possible to get slightly higher data rates
- **both** - supports both - short and long preamble

**prism-cardtype** (*30mW* | *100mW* | *200mW*) - specify the output of the Prism chipset based card

**proprietary-extensions** (*pre-2.9.25* | *post-2.9.25*; default: **post-2.9.25**) - the method to insert additional information (MikroTik proprietary extensions) into the wireless frames. This option is needed to workaround incompatibility between the old (pre-2.9.25) method and new Intel Centrino PCI-Express cards

- **pre-2.9.25** - include extensions in the form accepted by older RouterOS versions. This will include the new format as well, so this mode is compatible with all RouterOS versions. This mode is incompatible with wireless clients built on the new Centrino wireless chipset and may as well be incompatible with some other stations

**radio-name** (*text*) - descriptive name of the card. Only for MikroTik devices

**rate-set** (*default* | *configured*) - which rate set to use:

- **default** - basic and supported-rates settings are not used, instead default values are used
- **configured** - basic and supported-rates settings are used as configured

**scan-list** (*multiple choice: integer | default*; default: **default**) - the list of channels to scan

- **default** - represents all frequencies, allowed by the regulatory domain (in the respective country). If no country is set, these frequencies are used - for 2.4GHz mode: 2412, 2417, 2422, 2427, 2432, 2437, 2442, 2447, 2452, 2457, 2462; for 2.4GHz-g-turbo mode: 2437; for 5GHz mode: 5180, 5200, 5220, 5240, 5260, 5280, 5300, 5320, 5745, 5765, 5785, 5805, 5825; for 5GHz-turbo: 5210, 5250, 5290, 5760, 5800

**security-profile** (*text*; default: **default**) - which security profile to use. Define security profiles under /interface wireless security-profiles where you can setup WPA or WEP wireless security, for further details, see the Security Profiles section of this manual

**ssid** (*text*; default: **MikroTik**) - Service Set Identifier. Used to separate wireless networks

**supported-rates-a/g** (*multiple choice: 6Mbps, 9Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps*) - rates to be supported in 802.11a or 802.11g standard

**supported-rates-b** (*multiple choice: 1Mbps, 2Mbps, 5.5Mbps, 11Mbps*) - rates to be supported in 802.11b standard

**tx-power** (*integer: -30..30*; default: **17**) - manually sets the transmit power of the card (in dBm), if tx-power-mode is set to card rates or all-rates-fixed (see tx-power-mode description below)

**tx-power-mode** (*all-rates-fixed | card-rates | default | manual-table*; default: **default**) - choose the transmit power mode for the card:

- **all-rates-fixed** - use one transmit power value for all rates, as configured in tx-power
- **card-rates** - use transmit power, that for different rates is calculated according the cards transmit power algorithm, which as an argument takes tx-power value
- **default** - use the default tx-power
- **manual-table** - use the transmit powers as defined in /interface wireless manual-tx-power-table

**update-stats-interval** (*time*) - how often to update (request from the clients) signal strength and ccq values in /interface wireless registration-table

**wds-cost-range** (*integer*; default: **50-150**) - range, within which the bridge port cost of the WDS links are adjusted. The calculations are based on the p-throughput value of the respective WDS interface, which represents estimated approximate rthroughput on the interface, which is mapped on the wds-cost-range scale so that bigger p-throughput would correspond to numerically lower port cost. The cost is recalculated every 20 seconds or when the p-throughput changes more than by 10% since the last recalculation

**wds-default-bridge** (*name*; default: **none**) - the default bridge for WDS interface. If you use dynamic WDS then it is very useful in cases when wds connection is reset - the newly created dynamic WDS interface will be put in this bridge

**wds-default-cost** (*integer*; default: **100**) - default bridge port cost of the WDS links

**wds-ignore-ssid** (*yes | no*; default: **no**) - if set to 'yes', the AP will create WDS links with any other AP in this frequency. If set to 'no' the ssid values must match on both APs

**wds-mode** (*disabled | dynamic | static*) - WDS mode:

- **disabled** - WDS interfaces are disabled
- **dynamic** - WDS interfaces are created 'on the fly'
- **static** - WDS interfaces are created manually

**wmm-support** (*disabled | enabled | required*) - whether to allow (or require) peer to use WMM extensions to provide basic quality of service

## Notes

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.

It is strongly suggested to leave basic rates at the lowest setting possible.

Using **compression**, the AP can serve approximately 50 clients with compression enabled!

Compression is supported only by Atheros wireless cards.

If **disable-running-check** value is set to **no**, the router determines whether the network interface is up and running - in order to show flag **R** for AP, one or more clients have to be registered to it, for station, it should be connected to an AP. If the interface does not appear as running (**R**), its route in the routing table is shown as **invalid**! If set to **yes**, the interface will always be shown as running.

On Atheros-based cards, encryption (WEP, WPA, etc.) does not work when compression is enabled.

The **tx-power** default setting is the maximum tx-power that the card can use. If you want to use larger tx-rates, you are able to set them, but **do it at your own risk**! Usually, you can use this parameter to reduce the **tx-power**.

In general tx-power controlling properties should be left at the default settings. Changing the default setting may help with some cards in some situations, but without testing, the most common result is degradation of range and throughput. Some of the problems that may occur are: (1) overheating of the power amplifier chip and the card which will cause lower efficiency and more data errors; (2) overdriving the amplifier which will cause more data errors; (3) excessive power usage for the card and this may overload the 3.3V power supply of the board that the card is located on resulting in voltage drop and reboot or excessive temperatures for the board.

For different versions of Atheros chipset there are different value range of **ack-timeout** property:

Chipset version	5ghz		5ghz-turbo		2ghz-b		2ghz-g	
	default	max	default	max	default	max	default	max
5000 (5.2GHz only)	30	204	22	102	N/A	N/A	N/A	N/A
5211 (802.11a/b)	30	409	22	204	109	409	N/A	N/A
5212 (802.11a/b/g)	25	409	22	204	30	409	52	409

If the wireless interfaces are put in **nstreme-dual-slave** mode, all configuration will take place in **/interface wireless nstreme-dual** submenu, described further on in this manual. In that case, configuration made in this submenu will be partially ignored. WDS cannot be used together with the Nstreme-dual.

Some options are not shown by default - use **print advanced** in the console or press the "Advanced Mode" button in Winbox to see all the parameters

## Example

This example shows how configure a wireless client.

To see current interface settings:

```
[admin@MikroTik] interface wireless> print
Flags: X - disabled, R - running
0   name="wlan1" mtu=1500 mac-address=00:0C:42:18:5C:3D arp=enabled
    interface-type=Atheros AR5413 mode=station ssid="MikroTik" frequency=2412
    band=2.4ghz-b scan-list=default antenna-mode=ant-a wds-mode=disabled
    wds-default-bridge=none wds-ignore-ssid=no default-authentication=yes
    default-forwarding=yes default-ap-tx-limit=0 default-client-tx-limit=0
    hide-ssid=no security-profile=default compression=no
[admin@MikroTik] interface wireless>
```

Set the **ssid** to *mmt*, **band** to *2.4-b/g* and enable the interface. Use the monitor command to see the connection status.

```
[admin@MikroTik] interface wireless> set 0 ssid=mmt disabled=no \
band=2.4ghz-b/g
[admin@MikroTik] interface wireless> monitor wlan1
    status: connected-to-ess
        band: 2.4ghz-g
    frequency: 2412MHz
    tx-rate: "54Mbps"
    rx-rate: "54Mbps"
    ssid: "mmt"
    bssid: 00:0C:42:05:00:14
    radio-name: "000C42050014"
    signal-strength: -23dBm
    tx-signal-strength: -35dBm
    noise-floor: -96dBm
    signal-to-noise: 73dB
    tx-ccq: 79%
    rx-ccq: 46%
    p-throughput: 28681
    overall-tx-ccq: 79%
    authenticated-clients: 1
    current-ack-timeout: 56
        wds-link: no
        nstreme: no
        framing-mode: none
    routeros-version: "3.0"
        last-ip: 10.10.10.1
    802.1x-port-enabled: yes
    compression: no
    current-tx-powers: 1Mbps:19(19),2Mbps:19(19),5.5Mbps:19(19),
    11Mbps:19(19),6Mbps:19(19),9Mbps:19(19),
    12Mbps:19(19),18Mbps:19(19),24Mbps:19(19),
    36Mbps:18(18),48Mbps:17(17),54Mbps:16(16)
    notify-external-fdb: no
[admin@MikroTik] interface wireless>
```

The 'ess' stands for Extended Service Set (IEEE 802.11 wireless networking).

## Interface Monitor

Command name: */interface wireless monitor [interface name]*

### Description

With this command you can monitor your link information. It is very useful if you have established a wireless link and want to monitor its status.

### Property Description

**802.1x-port-enabled** (*read-only: yes | no*) - (on station only) whether the data exchange is allowed with the AP (i.e., whether 802.1x authentication is completed, if needed). Compare authenticated-clients and registered-clients

**authenticated-clients** (*read-only: integer*) - clients that have successfully completed 802.11 authentication process and have associated with the AP. Normally it is possible to exchange data with client right after this step, however WPA/WPA2 needs additional 802.1x authentication and dynamic key exchange procedures that start only after this stage (see registered-clients). For a wireless station this property relates to its AP

**band** - operating band

**bssid** (*read-only: MAC address*) - (on station only) MAC address of the AP

**compression** (*read-only: yes | no*) - (on station only) whether data compression is enabled for this interface

**current-ack-timeout** (*read-only: integer*) - current value of ack-timeout

**current-tx-powers** (*read-only: text*) - current transmit power values for every rate supported by the link

**framing-mode** (*read-only: text*) - (on station only) current framing mode

**frequency** (*read-only: integer*) - operating frequency

**last-ip** (*read-only: IP address*) - (on station only) source IP address found in the last IP packet received from the AP

**noise-floor** (*read-only: text*) - (on station only) received current noise level

**notify-external-fdb** (*read-only: yes | no*) - whether forwarding database is to be generated from the link's registration table to add known hosts in the local bridge host table (i.e., the associated bridge port is configured to request this information - its respective external-fdb property is set to auto or yes)

**nstreme** (*read-only: yes | no*) - whether nstreme protocol is used for this link

**overall-tx-ccq** (*read-only: integer*) - overall link CCQ, for transmitting to the wireless infrastructure, not to some particular peers

**p-throughput** (*read-only: integer*) - (on station only) estimated approximate throughput that is expected on the given link, by taking into account the effective transmit rate and hardware retries. Calculated once in 5 seconds

**radio-name** (*read-only: text*) - (on station only) radio name

**registered-clients** (*read-only: integer*) - (on AP only) number of fully authenticated clients, that have completed not only 802.11 authentication procedures (as specified in the authenticated-clients property), but also 802.1x ones. Registered clients are listed in the registration table and are ready for data exchange

**routeros-version** (*read-only: text*) - (on station only) RouterOS version installed on the AP

**rx-ccq** (*read-only: integer: 0..100*) - (on station only) Client Connection Quality - a value in percent that shows how effective the receive bandwidth (this value is received from the other end as this value represents its transmission quality) is used regarding the theoretically maximum available bandwidth. Mostly it depends from an amount of retransmitted wireless frames.

**rx-rate** (*read-only: text*) - (on station only) current receive air rate

**signal-strength** (*read-only: text*) - (on station only) received signal strength

**signal-to-noise** (*read-only: text*) - (on station only) signal to noise ratio

**ssid** (*read-only: text*) - (on station only) SSID

**status** (*read-only: searching-for-frequency | radar-detecting | running-ap | connected-to-ess | disabled*) - interface status

**tx-ccq** (*read-only: integer: 0..100*) - (on station only) Client Connection Quality - a value in percent that shows how effective the transmit bandwidth is used regarding the theoretically maximum available bandwidth. Mostly it depends from an amount of retransmitted wireless frames.

**tx-rate** (*read-only: text*) - (on station only) current transmit air rate

**tx-signal-strength** (*read-only: text*) - (on station only) received signal strength on the AP side (available if the AP is MikroTik RouterOS)

**wds-link** (*read-only: yes | no*) - (on station only) whether this link supports WDS (i.e., is in station-wds mode)

## Notes

Most values reported in station mode but absent for AP, are available in the registration table for particular stations connected to the AP.

## Nstreme Settings

Home menu level: */interface wireless nstreme*

### Description

You can switch a wireless card to the nstreme mode. In that case the card will work only with nstreme clients.

### Property Description

**disable-csma** (yes | no; default: **no**) - disable CSMA/CA when polling is used (better performance)

**enable-nstreme** (yes | no; default: **no**) - whether to switch the card into the nstreme mode

**enable-polling** (yes | no; default: **yes**) - whether to use polling for clients

**framer-limit** (*integer*; default: **3200**) - maximal frame size

**framer-policy** (*none | best-fit | exact-size | dynamic-size*; default: **none**) - the method how to combine frames. A number of frames may be combined into a bigger one to reduce the amount of protocol overhead (and thus increase speed). The card is not waiting for frames, but in case a number of packets are queued for transmitting, they can be combined. There are several methods of framing:

- **none** - do nothing special, do not combine packets (framing is disabled)
- **best-fit** - put as much packets as possible in one frame, until the framer-limit limit is met, but do not fragment packets
- **exact-size** - put as much packets as possible in one frame, until the framer-limit limit is met, even if fragmentation will be needed (best performance)
- **dynamic-size** - choose the best frame size dynamically

**name** (*name*) - reference name of the interface

## Notes

The settings here (except for enabling nstreme) are relevant only on Access Point, they are ignored for client devices! The client automatically adapts to the AP settings.

WDS for Nstreme protocol requires using station-wds mode on one of the peers. Configurations with WDS between AP modes (**bridge** and **ap-bridge**) will not work.

## Example

To enable the nstreme protocol on the **wlan1** radio with exact-size framing:

```
[admin@MikroTik] interface wireless nstreme> print
0 name="wlan1" enable-nstreme=no enable-polling=yes disable-csma=no
  framer-policy=none framer-limit=3200
[admin@MikroTik] interface wireless nstreme> set wlan1 enable-nstreme=yes \
\... framer-policy=exact-size
```

## Nstreme2 Group Settings

Home menu level: */interface wireless nstreme-dual*

### Description

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

### Property Description

**arp** (*disabled* | *enabled* | *proxy-arp* | *reply-only*; default: **enabled**) - Address Resolution Protocol setting

**disable-csma** (yes | no; default: **no**) - disable CSMA/CA (better performance)

**disable-running-check** (yes | no) - whether the interface should always be treated as running even if there is no connection to a remote peer

**framer-limit** (*integer*; default: **2560**) - maximal frame size

**framer-policy** (*none* | *best-fit* | *exact-size*; default: **none**) - the method how to combine frames. A

number of frames may be combined into one bigger one to reduce the amount of protocol overhead (and thus increase speed). The cards are not waiting for frames, but in case a number of packets are queued for transmitting, they can be combined. There are several methods of framing:

- **none** - do nothing special, do not combine packets
- **best-fit** - put as much packets as possible in one frame, until the frame-limit limit is met, but do not fragment packets
- **exact-size** - put as much packets as possible in one frame, until the frame-limit limit is met, even if fragmentation will be needed (best performance)

**mac-address** (*read-only: MAC address*) - MAC address of the transmitting wireless card in the set

**mtu** (*integer: 0..1600; default: 1500*) - Maximum Transmission Unit

**name** (*name*) - reference name of the interface

**rates-a/g** (*multiple choice: 6Mbps, 9Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps*) - rates to be supported in 802.11a or 802.11g standard

**rates-b** (*multiple choice: 1Mbps, 2Mbps, 5.5Mbps, 11Mbps*) - rates to be supported in 802.11b standard

**remote-mac** (*MAC address; default: 00:00:00:00:00:00*) - which MAC address to connect to (this would be the remote receiver card's MAC address)

**rx-band** - operating band of the receiving radio

- **2.4ghz-b** - IEEE 802.11b
- **2.4ghz-g** - IEEE 802.11g
- **2.4ghz-g-turbo** - IEEE 802.11g in Atheros proprietary turbo mode (up to 108Mbit)
- **5ghz** - IEEE 802.11a up to 54 Mbit
- **5ghz-turbo** - IEEE 802.11a in Atheros proprietary turbo mode (up to 108Mbit)
- **2ghz-10mhz** - variation of IEEE 802.11g with half the band, and, accordingly, twice lower speed (air rate of up to 27Mbit)
- **2ghz-5mhz** - variation of IEEE 802.11g with quarter the band, and, accordingly, four times lower speed (air rate of up to 13.5Mbit)
- **5ghz-10mhz** - variation of IEEE 802.11a with half the band, and, accordingly, twice lower speed (air rate of up to 27Mbit)
- **5ghz-5mhz** - variation of IEEE 802.11a with quarter the band, and, accordingly, four times lower speed (air rate of up to 13.5Mbit)

**rx-frequency** (*integer; default: 5320*) - Frequency to use for receiving frames

**rx-radio** (*name*) - which radio should be used for receiving frames

**tx-band** - operating band of the transmitting radio

- **2.4ghz-b** - IEEE 802.11b
- **2.4ghz-g** - IEEE 802.11g
- **2.4ghz-g-turbo** - IEEE 802.11g in Atheros proprietary turbo mode (up to 108Mbit)
- **5ghz** - IEEE 802.11a up to 54 Mbit
- **5ghz-turbo** - IEEE 802.11a in Atheros proprietary turbo mode (up to 108Mbit)
- **2ghz-10mhz** - variation of IEEE 802.11g with half the band, and, accordingly, twice lower speed (air rate of up to 27Mbit)

- **2ghz-5mhz** - variation of IEEE 802.11g with quarter the band, and, accordingly, four times lower speed (air rate of up to 13.5Mbit)
- **5ghz-10mhz** - variation of IEEE 802.11a with half the band, and, accordingly, twice lower speed (air rate of up to 27Mbit)
- **5ghz-5mhz** - variation of IEEE 802.11a with quarter the band, and, accordingly, four times lower speed (air rate of up to 13.5Mbit)

**tx-frequency** (*integer*; default: **5180**) - Frequency to use for transmitting frames

**tx-radio** (*name*) - which radio should be used for transmitting frames

## Notes

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 **2.4ghz-b** band.

## Example

To enable the nstreme2 protocol on a router:

1. Having two Atheros based cards which are not used for anything else, to group them into a nstreme interface, switch both of them into **nstreme-dual-slave** mode:

```
[admin@MikroTik] interface wireless> print
Flags: X - disabled, R - running
 0 R name="wlan1" mtu=1500 mac-address=00:0C:42:05:00:14 arp=enabled
   interface-type=Atheros AR5413 mode=station ssid="MikroTik"
   frequency=2412 band=2.4ghz-b/g scan-list=default antenna-mode=ant-a
   wds-mode=disabled wds-default-bridge=none wds-ignore-ssid=no
   default-authentication=yes default-forwarding=yes
   default-ap-tx-limit=0 default-client-tx-limit=0 hide-ssid=no
   security-profile=default compression=no

 1 name="wlan2" mtu=1500 mac-address=00:80:48:41:AF:2A arp=enabled
   interface-type=Atheros AR5413 mode=station ssid="MikroTik" frequency=2412
   band=2.4ghz-b/g scan-list=default antenna-mode=ant-a wds-mode=disabled
   wds-default-bridge=none wds-ignore-ssid=no default-authentication=yes
   default-forwarding=yes default-ap-tx-limit=0 default-client-tx-limit=0
   hide-ssid=no security-profile=default compression=no
[admin@MikroTik] interface wireless> set 0,1 mode=nstreme-dual-slave
```

2. Then add nstreme2 interface with exact-size framing:

```
[admin@MikroTik] interface wireless nstreme-dual> add \
...\ framer-policy=exact-size
```

3. Configure which card will be receiving and which - transmitting and specify remote receiver card's MAC address:

```
[admin@MikroTik] interface wireless nstreme-dual> print
Flags: X - disabled, R - running
```

```

0 X name="n-stremel" mtu=1500 mac-address=00:00:00:00:00:00 arp=enabled
  disable-running-check=no tx-radio=(unknown) rx-radio=(unknown)
  remote-mac=00:00:00:00:00:00 tx-band=5GHz tx-frequency=5180
  rx-band=5GHz rx-frequency=5320 disable-csma=no
  rates-b=1Mbps,2Mbps,5.5Mbps,11Mbps
  rates-a/g=6Mbps,9Mbps,12Mbps,18Mbps,24Mbps,36Mbps,48Mbps,54Mbps
  framer-policy=exact-size framer-limit=4000
[admin@MikroTik] interface wireless nstreme-dual> set 0 disabled=no \
\... tx-radio=wlan1 rx-radio=wlan2 remote-mac=00:0C:42:05:0B:12
[admin@MikroTik] interface wireless nstreme-dual> print
Flags: X - disabled, R - running
0 R name="n-stremel" mtu=1500 mac-address=00:0C:42:05:0B:12 arp=enabled
  disable-running-check=no tx-radio=wlan1 rx-radio=wlan2
  remote-mac=00:00:00:00:00:00 tx-band=5GHz tx-frequency=5180
  rx-band=5GHz rx-frequency=5320 disable-csma=no
  rates-b=1Mbps,2Mbps,5.5Mbps,11Mbps
  rates-a/g=6Mbps,9Mbps,12Mbps,18Mbps,24Mbps,36Mbps,48Mbps,54Mbps
  framer-policy=exact-size framer-limit=4000
[admin@MikroTik] interface wireless nstreme-dual>

```

## Registration Table

Home menu level: */interface wireless registration-table*

### Description

In the registration table you can see various information about currently connected clients. It is used only for Access Points.

### Property Description

**802.1x-port-enabled** (*read-only: yes | no*) - whether the data exchange is allowed with the peer (i.e., whether 802.1x authentication is completed, if needed)

**ack-timeout** (*read-only: integer*) - current value of ack-timeout

**ap** (*read-only: yes | no*) - whether the connected device is an Access Point or not

**ap-tx-limit** (*read-only: integer*) - transmit rate limit on the AP, in bits per second

**authentication-type** (*read-only: none | wpa-psk | wpa2-psk | wpa-eap | wpa2-eap*) - authentication method used for the peer

**bytes** (*read-only: integer, integer*) - number of sent and received packet bytes

**client-tx-limit** (*read-only: integer*) - transmit rate limit on the AP, in bits per second

**compression** (*read-only: yes | no*) - whether data compression is used for this peer

**encryption** (*read-only: aes-ccm | tkip*) - unicast encryption algorithm used

**frame-bytes** (*read-only: integer, integer*) - number of sent and received data bytes excluding header information

**frames** (*read-only: integer, integer*) - number of sent and received 802.11 data frames excluding retransmitted data frames

**framing-current-size** (*read-only: integer*) - current size of combined frames

**framing-limit** (*read-only: integer*) - maximal size of combined frames

**framing-mode** (*read-only: none | best-fit | exact-size; default: none*) - the method how to combine frames

**group-encryption** (*read-only: aes-ccm | tkip*) - group encryption algorithm used

**hw-frame-bytes** (*read-only: integer, integer*) - number of sent and received data bytes including header information

**hw-frames** (*read-only: integer, integer*) - number of sent and received 802.11 data frames including retransmitted data frames

**interface** (*read-only: name*) - interface that client is registered to

**last-activity** (*read-only: time*) - last interface data tx/rx activity

**last-ip** (*read-only: IP address*) - IP address found in the last IP packet received from the registered client

**mac-address** (*read-only: MAC address*) - MAC address of the registered client

**nstreme** (*read-only: yes | no*) - whether nstreme protocol is used for this link

**p-throughput** (*read-only: integer*) - estimated approximate throughput that is expected to the given peer, taking into account the effective transmit rate and hardware retries. Calculated once in 5 seconds

**packed-bytes** (*read-only: integer, integer*) - number of bytes packed into larger frames for transmitting/receiving (framing)

**packed-frames** (*read-only: integer, integer*) - number of frames packed into larger ones for transmitting/receiving (framing)

**packets** (*read-only: integer, integer*) - number of sent and received network layer packets

**radio-name** (*read-only: text*) - radio name of the peer

**routeros-version** (*read-only: name*) - RouterOS version of the registered client

**rx-ccq** (*read-only: integer: 0..100*) - Client Connection Quality - a value in percent that shows how effective the receive bandwidth is used regarding the theoretically maximum available bandwidth. Mostly it depends from an amount of retransmitted wireless frames.

**rx-rate** (*read-only: integer*) - receive data rate

**signal-strength** (*read-only: integer*) - average strength of the client signal received by the AP

**signal-to-noise** (*read-only: text*) - signal to noise ratio

**strength-at-rates** (*read-only: text*) - signal strength level at different rates together with time how long were these rates used

**tx-ccq** (*read-only: integer: 0..100*) - Client Connection Quality - a value in percent that shows how effective the transmit bandwidth is used regarding the theoretically maximum available bandwidth. Mostly it depends from an amount of retransmitted wireless frames.

**tx-frames-timed-out** (*read-only: integer*) - number of frames that have been discarded due to frame-lifetime timeout

**tx-rate** (*read-only: integer*) - transmit data rate

**tx-signal-strength** (*read-only: integer*) - average power of the AP transmit signal as received by the client device

**uptime** (*read-only: time*) - time the client is associated with the access point

**wds** (*read-only: no | yes*) - whether the connected client is using wds or not

**wmm-enabled** (*read-only: yes | no*) - whether WMM is used with this peer

## Example

To see registration table showing all clients currently associated with the access point:

```
[admin@MikroTik] interface wireless registration-table> print
# INTERFACE          RADIO-NAME          MAC-ADDRESS          AP  SIGNAL...  TX-RATE
0 wlan1              000C42185C3D       00:0C:42:18:5C:3D   no  -38dBm...  54Mbps
[admin@MikroTik] interface wireless registration-table>
```

To get additional statistics:

```
[admin@MikroTik] interface wireless> registration-table print stats
0 interface=wlan1 radio-name="000C42185C3D" mac-address=00:0C:42:18:5C:3D
ap=no wds=no rx-rate="1Mbps" tx-rate="54Mbps" packets=696,4147
bytes=5589,96698 frames=696,4147 frame-bytes=5589,71816
hw-frames=770,4162 hw-frame-bytes=24661,171784 tx-frames-timed-out=0
uptime=3h50m35s last-activity=2s440ms signal-strength=-38dBm@1Mbps
signal-to-noise=54dB
strength-at-rates=-38dBm@1Mbps 2s440ms,-37dBm@2Mbps 3h50m35s180ms,-
37dBm@5.5Mbps 3h50m23s330ms,-36dBm@11Mbps 3h45m8s330ms,-
37dBm@9Mbps 3h44m13s340ms,-36dBm@12Mbps 3h43m55s170ms,-
36dBm@18Mbps 3h43m43s340ms,-36dBm@24Mbps 3h43m25s180ms,-
37dBm@36Mbps 3h43m8s130ms,-42dBm@48Mbps 55s180ms,-
41dBm@54Mbps 3s610ms
tx-signal-strength=-43dBm tx-ccq=66% rx-ccq=88% p-throughput=30119
ack-timeout=56 nstreme=no framing-mode=none routeros-version="3.0"
ap-tx-limit=0 client-tx-limit=0 802.1x-port-enabled=yes compression=no
wmm-enabled=no
[admin@MikroTik] interface wireless>
```

## Connect List

Home menu level: */interface wireless connect-list*

### Description

The Connect List is a list of rules (order is important), that determine to which AP the station should connect to.

At first, the station is searching for APs all frequencies (from **scan-list**) in the respective band and makes a list of Access Points. If the **ssid** is set under **/interface wireless**, the router removes all Access Points from its AP list which do not have such **ssid**

If a rule is matched and the parameter **connect** is set to **yes**, the station will connect to this AP. If the parameter says **connect=no** or the rule is not matched, we jump to the next rule.

If we have gone through all rules and haven't connected to any AP, yet. The router chooses an AP with the best signal and **ssid** that is set under **/interface wireless**.

In case when the station has not connected to any AP, this process repeats from beginning.

### Property Description

**area-prefix** (*text*) - a string that indicates the beginning from the area string of the AP. If the AP's area begins with area-prefix, then this parameter returns true

**connect** (yes | no) - whether to connect to AP that matches this rule

**interface** (*name*) - name of the wireless interface

**mac-address** (*MAC address*) - MAC address of the AP. If set to 00:00:00:00:00:00, all APs are accepted

**security-profile** (*name*; default: **none**) - name of the security profile, used to connect to the AP. If none, then those security profile is used which is configured for the respective interface

**signal-range** (*integer*) - signal strength range in dBm. Rule is matched, if the signal from AP is within this range

**ssid** (*text*) - the ssid of the AP. If none set, all ssid's are accepted. Different ssids will be meaningful, if the ssid for the respective interface is set to ""

## Access List

Home menu level: */interface wireless access-list*

## Description

The access list is used by the Access Point to restrict associations of clients. This list contains MAC addresses of clients and determines what action to take when client attempts to connect. Also, the forwarding of frames sent by the client is controlled. Note that is is an ordered list (i.e., checked from top to bottom).

The association procedure is as follows: when a new client wants to associate to the AP that is configured on interface **wlanN**, an entry with client's MAC address and interface **wlanN** is looked up sequentially from top to bottom in the access-list. If such entry is found, action specified in the access list is performed, else **default-authentication** and **default-forwarding** arguments of interface **wlanN** are taken.

## Property Description

**ap-tx-limit** (*integer*; default: **0**) - limits data rate for this wireless client (in bps)

- **0** - no limits

**authentication** (*yes | no*; default: **yes**) - whether to accept or to reject this client when it tries to connect

**client-tx-limit** (*integer*; default: **0**) - limits this client's transmit data rate (in bps). Works only if the client is also a MikroTik Router

- **0** - no limits

**forwarding** (*yes | no*; default: **yes**) - whether to forward the client's frames to other wireless clients

**interface** (*name*) - name of the respective interface

**mac-address** (*MAC address*) - MAC address of the client (can be 00:00:00:00:00:00 for any client)

**private-algo** (*104bit-wep | 40bit-wep | none*) - which encryption algorithm to use

**private-key** (*text*; default: **""**) - private key of the client. Used for private-algo

**private-pre-shared-key** (*text*) - private preshared key for that station (in case any of the PSK authentication methods were used)

**signal-range** (*integer*) - signal strength range in dBm. Rule is matched, if the signal from AP is within this range

**time** (*time*) - rule is only matched during the specified period of time

## Notes

If you have default authentication action for the interface set to yes, you can disallow this node to register at

the AP's interface wlanN by setting authentication=no for it. Thus, all nodes except this one will be able to register to the interface wlanN.

If you have default authentication action for the interface set to no, you can allow this node to register at the AP's interface wlanN by setting authentication=yes for it. Thus, only the specified nodes will be able to register to the interface wlanN.

## Example

To allow authentication and forwarding for the client 00:01:24:70:3A:BB from the wlan1 interface using WEP 40bit algorithm with the key **1234567890**:

```
[admin@MikroTik] interface wireless access-list> add mac-address= \
...\ 00:01:24:70:3A:BB interface=wlan1 private-algo=40bit-wep private-key=1234567890
[admin@MikroTik] interface wireless access-list> print
Flags: X - disabled
0 mac-address=00:01:24:70:3A:BB interface=wlan1 signal-range=-120.120
  authentication=yes forwarding=yes ap-tx-limit=0 client-tx-limit=0
  private-algo=40bit-wep private-key="1234567890" private-pre-shared-key=""
[admin@MikroTik] interface wireless access-list>
```

## Info

Home menu level: */interface wireless info*

## Description

This facility provides you with general wireless interface information.

## Property Description

**2ghz-b-channels** (*multiple choice, read-only: 2312, 2317, 2322, 2327, 2332, 2337, 2342, 2347, 2352, 2357, 2362, 2367, 2372, 2412, 2417, 2422, 2427, 2432, 2437, 2442, 2447, 2452, 2457, 2462, 2467, 2472, 2484, 2512, 2532, 2552, 2572, 2592, 2612, 2632, 2652, 2672, 2692, 2712, 2732*) - the list of 2GHz IEEE 802.11b channels (frequencies are given in MHz)

**2ghz-g-channels** (*multiple choice, read-only: 2312, 2317, 2322, 2327, 2332, 2337, 2342, 2347, 2352, 2357, 2362, 2367, 2372, 2412, 2417, 2422, 2427, 2432, 2437, 2442, 2447, 2452, 2457, 2462, 2467, 2472, 2512, 2532, 2552, 2572, 2592, 2612, 2632, 2652, 2672, 2692, 2712, 2732, 2484*) - the list of 2GHz IEEE 802.11g channels (frequencies are given in MHz)

**5ghz-channels** (*multiple choice, read-only: 4920, 4925, 4930, 4935, 4940, 4945, 4950, 4955, 4960, 4965, 4970, 4975, 4980, 4985, 4990, 4995, 5000, 5005, 5010, 5015, 5020, 5025, 5030, 5035, 5040, 5045, 5050, 5055, 5060, 5065, 5070, 5075, 5080, 5085, 5090, 5095, 5100, 5105, 5110, 5115, 5120, 5125, 5130, 5135, 5140, 5145, 5150, 5155, 5160, 5165, 5170, 5175, 5180, 5185, 5190, 5195, 5200, 5205, 5210, 5215, 5220, 5225, 5230, 5235, 5240, 5245, 5250, 5255, 5260, 5265, 5270, 5275, 5280, 5285, 5290, 5295, 5300, 5305, 5310, 5315, 5320, 5325, 5330, 5335, 5340, 5345, 5350, 5355, 5360, 5365, 5370, 5375, 5380, 5385, 5390, 5395, 5400, 5405, 5410, 5415, 5420, 5425, 5430, 5435, 5440, 5445, 5450, 5455, 5460, 5465, 5470, 5475, 5480, 5485, 5490, 5495, 5500, 5505, 5510, 5515, 5520, 5525, 5530, 5535, 5540, 5545, 5550, 5555, 5560, 5565, 5570, 5575, 5580, 5585, 5590, 5595, 5600, 5605, 5610, 5615, 5620, 5625, 5630, 5635, 5640, 5645, 5650, 5655, 5660, 5665, 5670, 5675, 5680, 5685, 5690, 5695, 5700, 5705, 5710, 5715, 5720, 5725, 5730, 5735, 5740, 5745, 5750, 5755, 5760, 5765, 5770, 5775, 5780, 5785, 5790, 5795, 5800, 5805, 5810, 5815, 5820, 5825, 5830, 5835, 5840,*

5845, 5850, 5855, 5860, 5865, 5870, 5875, 5880, 5885, 5890, 5895, 5900, 5905, 5910, 5915, 5920, 5925, 5930, 5935, 5940, 5945, 5950, 5955, 5960, 5965, 5970, 5975, 5980, 5985, 5990, 5995, 6000, 6005, 6010, 6015, 6020, 6025, 6030, 6035, 6040, 6045, 6050, 6055, 6060, 6065, 6070, 6075, 6080, 6085, 6090, 6095, 6100) - the list of 5GHz channels (frequencies are given in MHz)

**5ghz-turbo-channels** (*multiple choice, read-only: 4920, 4925, 4930, 4935, 4940, 4945, 4950, 4955, 4960, 4965, 4970, 4975, 4980, 4985, 4990, 4995, 5000, 5005, 5010, 5015, 5020, 5025, 5030, 5035, 5040, 5045, 5050, 5055, 5060, 5065, 5070, 5075, 5080, 5085, 5090, 5095, 5100, 5105, 5110, 5115, 5120, 5125, 5130, 5135, 5140, 5145, 5150, 5155, 5160, 5165, 5170, 5175, 5180, 5185, 5190, 5195, 5200, 5205, 5210, 5215, 5220, 5225, 5230, 5235, 5240, 5245, 5250, 5255, 5260, 5265, 5270, 5275, 5280, 5285, 5290, 5295, 5300, 5305, 5310, 5315, 5320, 5325, 5330, 5335, 5340, 5345, 5350, 5355, 5360, 5365, 5370, 5375, 5380, 5385, 5390, 5395, 5400, 5405, 5410, 5415, 5420, 5425, 5430, 5435, 5440, 5445, 5450, 5455, 5460, 5465, 5470, 5475, 5480, 5485, 5490, 5495, 5500, 5505, 5510, 5515, 5520, 5525, 5530, 5535, 5540, 5545, 5550, 5555, 5560, 5565, 5570, 5575, 5580, 5585, 5590, 5595, 5600, 5605, 5610, 5615, 5620, 5625, 5630, 5635, 5640, 5645, 5650, 5655, 5660, 5665, 5670, 5675, 5680, 5685, 5690, 5695, 5700, 5705, 5710, 5715, 5720, 5725, 5730, 5735, 5740, 5745, 5750, 5755, 5760, 5765, 5770, 5775, 5780, 5785, 5790, 5795, 5800, 5805, 5810, 5815, 5820, 5825, 5830, 5835, 5840, 5845, 5850, 5855, 5860, 5865, 5870, 5875, 5880, 5885, 5890, 5895, 5900, 5905, 5910, 5915, 5920, 5925, 5930, 5935, 5940, 5945, 5950, 5955, 5960, 5965, 5970, 5975, 5980, 5985, 5990, 5995, 6000, 6005, 6010, 6015, 6020, 6025, 6030, 6035, 6040, 6045, 6050, 6055, 6060, 6065, 6070, 6075, 6080, 6085, 6090, 6095, 6100*) - the list of 5GHz-turbo channels (frequencies are given in MHz)

**ack-timeout-control** (*read-only: yes | no*) - provides information whether this device supports transmission acceptance timeout control

**alignment-mode** (*read-only: yes | no*) - is the alignment-only mode supported by this interface

**burst-support** (*yes | no*) - whether the interface supports data bursts (burst-time)

**chip-info** (*read-only: text*) - information from EEPROM

**default-periodic-calibration** (*read-only: yes | no*) - whether the card supports periodic-calibration

**firmware** (*read-only: text*) - current firmware of the interface (used only for Prism chipset based cards)

**interface-type** (*read-only: text*) - shows the hardware interface type

**noise-floor-control** (*read-only: yes | no*) - does this interface support noise-floor-threshold detection

**nstreme-support** (*read-only: yes | no*) - whether the card supports n-streme protocol

**scan-support** (*yes | no*) - whether the interface supports scan function ('/interface wireless scan')

**supported-bands** (*multiple choice, read-only: 2ghz-b, 5ghz, 5ghz-turbo, 2ghz-g*) - the list of supported bands

**tx-power-control** (*read-only: yes | no*) - provides information whether this device supports transmission power control

**virtual-aps** (*read-only: yes | no*) - whether this interface supports Virtual Access Points ('/interface wireless add')

## Notes

There is a special argument for the print command - print count-only. It forces the print command to print only the count of information topics.

/interface wireless info print command shows only channels supported by a particular card.

### Example

```
[admin@MikroTik] interface wireless info> print
 0 interface-type=Atheros AR5413 chip-info="mac:0xa/0x5, phy:0x61, a5:0x63, a2:0x0,
eeprom:0x5002" pci-info="00:04.0"
capabilities=tx-power-control,ack-timeout-control,virtual-ap,alignment-mode,noise-floor-control,scann
power-channel,wmm
default-periodic-calibration=enabled
supported-bands=2ghz-b,5ghz,5ghz-turbo,2ghz-g,2ghz-g-turbo,5ghz-10mhz,5ghz-5mhz,2ghz-10mhz,2ghz-5mhz
2ghz-b-channels=2192:0,2197:0,2202:0,2207:0,2212:0,2217:0,2222:0,2227:0,2232:0,2237:0,2242:0,2247:0,2
2287:0,2292:0,2297:0,2302:0,2307:0,2312:0,2317:0,2322:0,2327:0,2332:0,2337:0,2342:0,2347:0,2352:0,235
2382:0,2387:0,2392:0,2397:0,2402:0,2407:0,2412:0,2417:0,2422:0,2427:0,2432:0,2437:0,2442:0,2447:0,245
2477:0,2482:0,2487:0,2492:0,2497:0,2502:0,2507:0,2224:0,2229:0,2234:0,2239:0,2244:0,2249:0,2254:0,225
2284:0,2289:0,2294:0,2299:0,2304:0,2309:0,2314:0,2319:0,2324:0,2329:0,2334:0,2339:0,2344:0,2349:0,235
2379:0,2384:0,2389:0,2394:0,2399:0,2404:0,2409:0,2414:0,2419:0,2424:0,2429:0,2434:0,2439:0,2444:0,244
2474:0,2479:0,2484:0,2489:0,2494:0,2499:0,2504:0,2509:0,2514:0,2519:0,2524:0,2529:0,2534:0,2539:0
5ghz-channels=4920:0,4925:0,4930:0,4935:0,4940:0,4945:0,4950:0,4955:0,4960:0,4965:0,4970:0,4975:0,498
5015:0,5020:0,5025:0,5030:0,5035:0,5040:0,5045:0,5050:0,5055:0,5060:0,5065:0,5070:0,5075:0,5080:0,508
5110:0,5115:0,5120:0,5125:0,5130:0,5135:0,5140:0,5145:0,5150:0,5155:0,5160:0,5165:0,5170:0,5175:0,518
5205:0,5210:0,5215:0,5220:0,5225:0,5230:0,5235:0,5240:0,5245:0,5250:0,5255:0,5260:0,5265:0,5270:0,527
5300:0,5305:0,5310:0,5315:0,5320:0,5325:0,5330:0,5335:0,5340:0,5345:0,5350:0,5355:0,5360:0,5365:0,537
5395:0,5400:0,5405:0,5410:0,5415:0,5420:0,5425:0,5430:0,5435:0,5440:0,5445:0,5450:0,5455:0,5460:0,546
5490:0,5495:0,5500:0,5505:0,5510:0,5515:0,5520:0,5525:0,5530:0,5535:0,5540:0,5545:0,5550:0,5555:0,556
5585:0,5590:0,5595:0,5600:0,5605:0,5610:0,5615:0,5620:0,5625:0,5630:0,5635:0,5640:0,5645:0,5650:0,565
5680:0,5685:0,5690:0,5695:0,5700:0,5705:0,5710:0,5715:0,5720:0,5725:0,5730:0,5735:0,5740:0,5745:0,575
5775:0,5780:0,5785:0,5790:0,5795:0,5800:0,5805:0,5810:0,5815:0,5820:0,5825:0,5830:0,5835:0,5840:0,584
5870:0,5875:0,5880:0,5885:0,5890:0,5895:0,5900:0,5905:0,5910:0,5915:0,5920:0,5925:0,5930:0,5935:0,594
5965:0,5970:0,5975:0,5980:0,5985:0,5990:0,5995:0,6000:0,6005:0,6010:0,6015:0,6020:0,6025:0,6030:0,603
6060:0,6065:0,6070:0,6075:0,6080:0,6085:0,6090:0,6095:0,6100:0
5ghz-turbo-channels=4920:0,4925:0,4930:0,4935:0,4940:0,4945:0,4950:0,4955:0,4960:0,4965:0,4970:0,4975
5015:0,5020:0,5025:0,5030:0,5035:0,5040:0,5045:0,5050:0,5055:0,5060:0,5065:0,5070:0,5075:0,5080:0,508
5110:0,5115:0,5120:0,5125:0,5130:0,5135:0,5140:0,5145:0,5150:0,5155:0,5160:0,5165:0,5170:0,5175:0,518
5205:0,5210:0,5215:0,5220:0,5225:0,5230:0,5235:0,5240:0,5245:0,5250:0,5255:0,5260:0,5265:0,5270:0,527
5300:0,5305:0,5310:0,5315:0,5320:0,5325:0,5330:0,5335:0,5340:0,5345:0,5350:0,5355:0,5360:0,5365:0,537
5395:0,5400:0,5405:0,5410:0,5415:0,5420:0,5425:0,5430:0,5435:0,5440:0,5445:0,5450:0,5455:0,5460:0,546
5490:0,5495:0,5500:0,5505:0,5510:0,5515:0,5520:0,5525:0,5530:0,5535:0,5540:0,5545:0,5550:0,5555:0,556
5585:0,5590:0,5595:0,5600:0,5605:0,5610:0,5615:0,5620:0,5625:0,5630:0,5635:0,5640:0,5645:0,5650:0,565
5680:0,5685:0,5690:0,5695:0,5700:0,5705:0,5710:0,5715:0,5720:0,5725:0,5730:0,5735:0,5740:0,5745:0,575
5775:0,5780:0,5785:0,5790:0,5795:0,5800:0,5805:0,5810:0,5815:0,5820:0,5825:0,5830:0,5835:0,5840:0,584
5870:0,5875:0,5880:0,5885:0,5890:0,5895:0,5900:0,5905:0,5910:0,5915:0,5920:0,5925:0,5930:0,5935:0,594
5965:0,5970:0,5975:0,5980:0,5985:0,5990:0,5995:0,6000:0,6005:0,6010:0,6015:0,6020:0,6025:0,6030:0,603
6060:0,6065:0,6070:0,6075:0,6080:0,6085:0,6090:0,6095:0,6100:0
2ghz-g-channels=2192:0,2197:0,2202:0,2207:0,2212:0,2217:0,2222:0,2227:0,2232:0,2237:0,2242:0,2247:0,2
2287:0,2292:0,2297:0,2302:0,2307:0,2312:0,2317:0,2322:0,2327:0,2332:0,2337:0,2342:0,2347:0,2352:0,235
2382:0,2387:0,2392:0,2397:0,2402:0,2407:0,2412:0,2417:0,2422:0,2427:0,2432:0,2437:0,2442:0,2447:0,245
2477:0,2482:0,2487:0,2492:0,2497:0,2502:0,2507:0,2224:0,2229:0,2234:0,2239:0,2244:0,2249:0,2254:0,225
2284:0,2289:0,2294:0,2299:0,2304:0,2309:0,2314:0,2319:0,2324:0,2329:0,2334:0,2339:0,2344:0,2349:0,235
2379:0,2384:0,2389:0,2394:0,2399:0,2404:0,2409:0,2414:0,2419:0,2424:0,2429:0,2434:0,2439:0,2444:0,244
2474:0,2479:0,2484:0,2489:0,2494:0,2499:0,2504:0,2509:0,2514:0,2519:0,2524:0,2529:0,2534:0,2539:0
2ghz-g-turbo-channels=2192:0,2197:0,2202:0,2207:0,2212:0,2217:0,2222:0,2227:0,2232:0,2237:0,2242:0,22
2282:0,2287:0,2292:0,2297:0,2302:0,2307:0,2312:0,2317:0,2322:0,2327:0,2332:0,2337:0,2342:0,2347:0,235
2372:0,2377:0,2382:0,2387:0,2392:0,2397:0,2402:0,2407:0,2412:0,2417:0,2422:0,2427:0,2432:0,2437:0,244
2462:0,2467:0,2472:0,2477:0,2482:0,2487:0,2492:0,2497:0,2502:0,2507:0,2224:0,2229:0,2234:0,2239:0,224
2264:0,2269:0,2274:0,2279:0,2284:0,2289:0,2294:0,2299:0,2304:0,2309:0,2314:0,2319:0,2324:0,2329:0,233
2354:0,2359:0,2364:0,2369:0,2374:0,2379:0,2384:0,2389:0,2394:0,2399:0,2404:0,2409:0,2414:0,2419:0,242
2444:0,2449:0,2454:0,2459:0,2464:0,2469:0,2474:0,2479:0,2484:0,2489:0,2494:0,2499:0,2504:0,2509:0,251
2534:0,2539:0
5ghz-10mhz-power-channels=4920:0,4925:0,4930:0,4935:0,4940:0,4945:0,4950:0,4955:0,4960:0,4965:0,4970:0
5010:0,5015:0,5020:0,5025:0,5030:0,5035:0,5040:0,5045:0,5050:0,5055:0,5060:0,5065:0,5070:0,5075:0,508
5100:0,5105:0,5110:0,5115:0,5120:0,5125:0,5130:0,5135:0,5140:0,5145:0,5150:0,5155:0,5160:0,5165:0,517
5190:0,5195:0,5200:0,5205:0,5210:0,5215:0,5220:0,5225:0,5230:0,5235:0,5240:0,5245:0,5250:0,5255:0,526
5280:0,5285:0,5290:0,5295:0,5300:0,5305:0,5310:0,5315:0,5320:0,5325:0,5330:0,5335:0,5340:0,5345:0,535
5370:0,5375:0,5380:0,5385:0,5390:0,5395:0,5400:0,5405:0,5410:0,5415:0,5420:0,5425:0,5430:0,5435:0,544
5460:0,5465:0,5470:0,5475:0,5480:0,5485:0,5490:0,5495:0,5500:0,5505:0,5510:0,5515:0,5520:0,5525:0,553
5550:0,5555:0,5560:0,5565:0,5570:0,5575:0,5580:0,5585:0,5590:0,5595:0,5600:0,5605:0,5610:0,5615:0,562
5640:0,5645:0,5650:0,5655:0,5660:0,5665:0,5670:0,5675:0,5680:0,5685:0,5690:0,5695:0,5700:0,5705:0,571
5730:0,5735:0,5740:0,5745:0,5750:0,5755:0,5760:0,5765:0,5770:0,5775:0,5780:0,5785:0,5790:0,5795:0,580
5820:0,5825:0,5830:0,5835:0,5840:0,5845:0,5850:0,5855:0,5860:0,5865:0,5870:0,5875:0,5880:0,5885:0,589
5910:0,5915:0,5920:0,5925:0,5930:0,5935:0,5940:0,5945:0,5950:0,5955:0,5960:0,5965:0,5970:0,5975:0,598
6000:0,6005:0,6010:0,6015:0,6020:0,6025:0,6030:0,6035:0,6040:0,6045:0,6050:0,6055:0,6060:0,6065:0,607
```



only if the client is also a MikroTik Router

- **0** - no limits

**default-forwarding** (*yes | no*; default: **yes**) - whether to forward frames to other AP clients or not

**disable-running-check** (*yes | no*; default: **no**) - disable running check. For 'broken' cards it is a good idea to set this value to 'yes'

**disabled** (*yes | no*; default: **yes**) - whether to disable the interface or not

**hide-ssid** (*yes | no*; default: **no**) - whether to hide ssid or not in the beacon frames:

- **yes** - ssid is not included in the beacon frames. AP replies only to probe-requests with the given ssid
- **no** - ssid is included in beacon frames. AP replies to probe-requests with the given ssid and to 'broadcast ssid'

**mac-address** (*MAC address*; default: **02:00:00:AA:00:00**) - MAC address of VAP. You can define your own value for mac-address

**master-interface** (*name*) - hardware interface to use for VAP

**max-station-count** (*integer*; default: **2007**) - number of clients that can connect to this AP simultaneously

**mtu** (*integer*: 68..1600; default: **1500**) - Maximum Transmission Unit

**name** (*name*; default: **wlanN**) - interface name

**proprietary-extensions** (*pre-2.9.25 | post-2.9.25*; default: **post-2.9.25**) - the method to insert additional information (MikroTik proprietary extensions) into the wireless frames. This option is needed to workaroud incompatibility between the old (pre-2.9.25) method and new Intel Centrino PCI-Express cards

- **pre-2.9.25** - include extensions in the form accepted by older RouterOS versions. This will include the new format as well, so this mode is compatible with all RouterOS versions. This mode is incompatible with wireless clients built on the new Centrino wireless chipset and may as well be incompatible with some other stations

**security-profile** (*text*; default: **default**) - which security profile to use. Define security profiles under /interface wireless security-profiles where you can setup WPA or WEP wireless security, for further details, see the Security Profiles section of this manual

**ssid** (*text*; default: **MikroTik**) - the service set identifier

**update-stats-interval** (*time*) - how often to update (request from the clients) signal strength and ccq values in /interface wireless registration-table

**wds-cost-range** (*integer*; default: **50-150**) - range, within which the bridge port cost of the WDS links are adjusted. The calculations are based on the p-throughput value of the respective WDS interface, which represents estimated approximate rhtoughput on the interface, which is mapped on the wds-cost-range scale so that bigger p-throughput would correspond to numerically lower port cost. The cost is recalculated every 20 seconds or when the p-throughput changes more than by 10% since the last recalculation

**wds-default-bridge** (*name*; default: **none**) - the default bridge for WDS interface. If you use dynamic WDS then it is very useful in cases when wds connection is reset - the newly created dynamic WDS interface will be put in this bridge

**wds-default-cost** (*integer*; default: **100**) - default bridge port cost of the WDS links

**wds-ignore-ssid** (*yes | no*; default: **no**) - if set to 'yes', the AP will create WDS links with any other

AP in this frequency. If set to 'no' the ssid values must match on both APs

**wds-mode** (*disabled* | *dynamic* | *static*) - WDS mode:

- **disabled** - WDS interfaces are disabled
- **dynamic** - WDS interfaces are created 'on the fly'
- **static** - WDS interfaces are created manually

**wmm-support** (*disabled* | *enabled* | *required*) - whether to allow (or require) peer to use WMM extensions to provide basic quality of service

## Notes

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.

## WDS Interface Configuration

Home menu level: */interface wireless wds*

### Description

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.

There are two possibilities to create a WDS interface:

- **dynamic** - is created 'on the fly' and appears under wds menu as a dynamic interface
- **static** - is created manually

### Property Description

**arp** (*disabled* | *enabled* | *proxy-arp* | *reply-only*; default: **enabled**) - Address Resolution Protocol

- **disabled** - the interface will not use ARP
- **enabled** - the interface will use ARP
- **proxy-arp** - the interface will use the ARP proxy feature
- **reply-only** - the interface will only reply to the requests originated to its own IP addresses. Neighbour MAC addresses will be resolved using /ip arp statically set table only

**disable-running-check** (*yes* | *no*; default: **no**) - disable running check. For 'broken' wireless cards it is a good idea to set this value to 'yes'

**mac-address** (*read-only: MAC address*; default: **00:00:00:00:00:00**) - MAC address of the master-interface. Specifying master-interface, this value will be set automatically

**master-interface** (*name*) - wireless interface which will be used by WDS

**mtu** (*integer*: 0..65536; default: **1500**) - Maximum Transmission Unit

**name** (*name*; default: **wdsN**) - WDS interface name

**wds-address** (*MAC address*) - MAC address of the remote WDS host

## Notes

When the link between WDS devices, using **wds-mode=dynamic**, goes down, the dynamic WDS interfaces disappear and if there are any IP addresses set on this interface, their 'interface' setting will change to **(unknown)**. When the link comes up again, the 'interface' value will not change - it will remain as **(unknown)**. That's why it is not recommended to add IP addresses to dynamic WDS interfaces.

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.

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.

WDS significantly faster than EoIP (up to 10-20% on RouterBOARD 500 systems), so it is recommended to use WDS whenever possible.

## Example

```
[admin@MikroTik] interface wireless wds> add master-interface=wlan1 \  
\... wds-address=00:0B:6B:30:2B:27 disabled=no  
[admin@MikroTik] interface wireless wds> print  
Flags: X - disabled, R - running, D - dynamic  
0 R name="wds1" mtu=1500 mac-address=00:0B:6B:30:2B:23 arp=enabled  
    disable-running-check=no master-inteface=wlan1  
    wds-address=00:0B:6B:30:2B:27  
[admin@MikroTik] interface wireless wds>
```

## Align

Home menu level: */interface wireless align*

## Description

This feature is created to position wireless links. The **align** submenu describes properties which are used if **/interface wireless mode** is set to **alignment-only**. In this mode the interface 'listens' to those packets which are sent to it from other devices working on the same channel. The interface also can send special packets which contains information about its parameters.

## Property Description

**active-mode** (*yes | no*; default: **yes**) - whether the interface will receive and transmit 'alignment' packets or it will only receive them

**audio-max** (*integer*; default: **-20**) - signal-strength at which audio (beeper) frequency will be the highest

**audio-min** (*integer*; default: **-100**) - signal-strength at which audio (beeper) frequency will be the

lowest

**audio-monitor** (*MAC address*; default: **00:00:00:00:00:00**) - MAC address of the remote host which will be 'listened'

**filter-mac** (*MAC address*; default: **00:00:00:00:00:00**) - in case if you want to receive packets from only one remote host, you should specify here its MAC address

**frame-size** (*integer*: 200..1500; default: **300**) - size of 'alignment' packets that will be transmitted

**frames-per-second** (*integer*: 1..100; default: **25**) - number of frames that will be sent per second (in active-mode)

**receive-all** (*yes | no*; default: **no**) - whether the interface gathers packets about other 802.11 standard packets or it will gather only 'alignment' packets

**ssid-all** (*yes | no*; default: **no**) - whether you want to accept packets from hosts with other ssid than yours

## Command Description

**test-audio** (*integer*) - test the beeper for 10 seconds

## Notes

If you are using the command **/interface wireless align monitor** then it will automatically change the wireless interface's mode from **station**, **bridge** or **ap-bridge** to **alignment-only**.

## Example

```
[admin@MikroTik] interface wireless align> print
  frame-size: 300
  active-mode: yes
  receive-all: yes
  audio-monitor: 00:00:00:00:00:00
  filter-mac: 00:00:00:00:00:00
  ssid-all: no
  frames-per-second: 25
  audio-min: -100
  audio-max: -20
[admin@MikroTik] interface wireless align>
```

## Align Monitor

Command name: **/interface wireless align monitor**

## Description

This command is used to monitor current signal parameters to/from a remote host.

## Property Description

**address** (*read-only: MAC address*) - MAC address of the remote host

**avg-rxq** (*read-only: integer*) - average signal strength of received packets since last display update on screen

**correct** (*read-only: percentage*) - how many undamaged packets were received

**last-rx** (*read-only: time*) - time in seconds before the last packet was received

**last-tx** (*read-only: time*) - time in seconds when the last TXQ info was received

**rxq** (*read-only: integer*) - signal strength of last received packet

**ssid** (*read-only: text*) - service set identifier

**txq** (*read-only: integer*) - the last received signal strength from our host to the remote one

## Example

```
[admin@MikroTik] interface wireless align> monitor wlan2
# ADDRESS          SSID          RXQ  AVG-RXQ  LAST-RX  TXQ  LAST-TX  CORRECT
0 00:01:24:70:4B:FC wirelesa    -60 -60      0.01   -67  0.01    100 %

[admin@MikroTik] interface wireless align>
```

## Frequency Monitor

Command name: */interface wireless frequency-monitor*

### Description

Aproximately shows how loaded are the wireless channels.

### Property Description

**freq** (*read-only: integer*) - shows current channel

**use** (*read-only: percentage*) - shows usage in current channel

## Example

Monitor 802.11b network load:

```
[admin@MikroTik] interface wireless> frequency-monitor wlan1

FREQ          USE
2412MHz       3.8%
2417MHz       9.8%
2422MHz       2%
2427MHz       0.8%
2432MHz       0%
2437MHz       0.9%
2442MHz       0.9%
2447MHz       2.4%
2452MHz       3.9%
2457MHz       7.5%
2462MHz       0.9%
```

To monitor other bands, change the the **band** setting for the respective wireless interface.

## Manual Transmit Power Table

Home menu level: */interface wireless manual-tx-power-table*

### Description

In this submenu you can define signal strength for each rate. You should be aware that you can damage your wireless card if you set higher output power than it is allowed. Note that the values in this table are set in **dBm!** **NOT in mW!** Therefore this table is used mainly to reduce the transmit power of the card.

## Property Description

**manual-tx-powers** (*text*) - define tx-power in dBm for each rate, separate by commas

## Example

To set the following transmit powers at each rates: 1Mbps@10dBm, 2Mbps@10dBm, 5.5Mbps@9dBm, 11Mbps@7dBm, do the following:

```
[admin@MikroTik] interface wireless manual-tx-power-table> print
0 name="wlan1" manual-tx-powers=1Mbps:17,2Mbps:17,5.5Mbps:17,11Mbps:17,6Mbps:17
,
          9Mbps:17,12Mbps:17,18Mbps:17,24Mbps:17,
          36Mbps:17,48Mbps:17,54Mbps:17

[admin@MikroTik] interface wireless manual-tx-power-table> set 0 \
manual-tx-powers=1Mbps:10,2Mbps:10,5.5Mbps:9,11Mbps:7

[admin@MikroTik] interface wireless manual-tx-power-table> print
0 name="wlan1" manual-tx-powers=1Mbps:10,2Mbps:10,5.5Mbps:9,11Mbps:7
[admin@MikroTik] interface wireless manual-tx-power-table>
```

## Network Scan

Command name: */interface wireless scan interface\_name*

## Description

This is a feature that allows you to scan all available wireless networks. 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.

## Property Description

**address** (*read-only: MAC address*) - MAC address of the AP

**band** (*read-only: text*) - in which standard does the AP operate

**bss** (*read-only: yes | no*) - basic service set

**freeze-time-interval** (*time; default: 1s*) - time in seconds to refresh the displayed data

**freq** (*read-only: integer*) - the frequency of AP

**interface\_name** (*name*) - the name of interface which will be used for scanning APs

**privacy** (*read-only: yes | no*) - whether all data is encrypted or not

**signal-strength** (*read-only: integer*) - signal strength in dBm

**ssid** (*read-only: text*) - service set identifier of the AP

## Example

Scan the 5GHz band:

```
[admin@MikroTik] interface wireless> scan wlan1
Flags: A - active, B - bss, P - privacy, R - routeros-network, N - nstreme
ADDRESS          SSID          BAND          FREQ SIG RADIO-NAME
AB R 00:0C:42:05:00:28 test          5ghz          5180 -77 000C42050028
AB R 00:02:6F:20:34:82 aapl          5ghz          5180 -73 00026F203482
AB   00:0B:6B:30:80:0F www           5ghz          5180 -84
AB R 00:0B:6B:31:B6:D7 www           5ghz          5180 -81 000B6B31B6D7
AB R 00:0B:6B:33:1A:D5 R52_test_new 5ghz          5180 -79 000B6B331AD5
AB R 00:0B:6B:33:0D:EA short5        5ghz          5180 -70 000B6B330DEA
AB R 00:0B:6B:31:52:69 MikroTik         5ghz          5220 -69 000B6B315269
AB R 00:0B:6B:33:12:BF long2           5ghz          5260 -55 000B6B3312BF
-- [Q quit|D dump|C-z pause]
[admin@MikroTik] interface wireless>
```

## Security Profiles

Home menu level: */interface wireless security-profiles*

### Description

This section provides WEP (Wired Equivalent Privacy) and WPA/WPA2 (Wi-Fi Protected Access) functions to wireless interfaces.

#### WPA

The Wi-Fi Protected Access is a combination of 802.1X, EAP, MIC, TKIP and AES. This is a easy to configure and secure wireless mechanism. It has been later updated to version 2, to provide greater security.

Pairwise master key caching for EAP authentication is supported for WPA2. This means that disconnected client can connect without repeated EAP authentication if keys are still valid (changed to interface or security profile configuration, restart, or Session-Timeout in case of RADIUS authentication).

#### WEP

The Wired Equivalent Privacy encrypts data only between 802.11 devices, using static keys. It is not considered a very secure wireless data encryption mechanism, though it is better than no encryption at all.

The configuration of WEP is quite simple, using MikroTik RouterOS security profiles.

### Property Description

**authentication-types** (*multiple choice: wpa-psk | wpa2-psk | wpa-eap | wpa2-eap*; default: "") - the list of accepted authentication types. APs will advertise the listed types. Stations will choose the AP, which supports the "best" type from the list (WPA2 is always preferred to WPA1; EAP is preferred to PSK)

**eap-methods** (*multiple choice: eap-tls | passthrough*) - the ordered list of EAP methods. APs will to propose to the stations one by one (if first method listed is rejected, the next one is tried). Stations will accept first proposed method that will be on the list

- **eap-tls** - Use TLS certificates for authentication
- **passthrough** - relay the authentication process to the RADIUS server (not used by the stations)

**group-ciphers** (*multiple choice: `tkip` | `aes-ccm`*) - a set of ciphers used to encrypt frames sent to all wireless station (broadcast transfers) in the order of preference

- **tkip** - Temporal Key Integrity Protocol - encryption protocol, compatible with legacy WEP equipment, but enhanced to correct some of WEP flaws
- **aes-ccm** - more secure WPA encryption protocol, based on the reliable AES (Advanced Encryption Standard). Networks free of WEP legacy should use only this

**group-key-update** (*time*; default: **5m**) - how often to update group key. This parameter is used only if the wireless card is configured as an Access Point

**interim-update** (*time*) - default update interval for RADIUS accounting, if RADIUS server has not provided different value

**mode** (*none | static-keys-optional | static-keys-required | dynamic-keys*; default: **none**) - security mode:

- **none** - do not encrypt packets and do not accept encrypted packets
- **static-keys-optional** - if there is a static-sta-private-key set, use it. Otherwise, if the interface is set in an AP mode, do not use encryption, if the the interface is in station mode, use encryption if the static-transmit-key is set
- **static-keys-required** - encrypt all packets and accept only encrypted packets
- **dynamic-keys** - generate encryption keys dynamically

**name** (*name*) - descriptive name for the security profile

**radius-eap-accounting** (*yes | no*; default: **no**) - use RADIUS accounting if EAP authentication is used

**radius-mac-accounting** (*yes | no*; default: **no**) - use RADIUS accounting, providing MAC address as username

**radius-mac-authentication** (*no | yes*; default: **no**) - whether to use RADIUS server for MAC authentication

**radius-mac-caching** (*time*; default: **disabled**) - how long the RADIUS authentication reply for MAC address authentication if considered valid (and thus can be cached for faster reauthentication)

**radius-mac-format** (*text*; default: **XX:XX:XX:XX:XX:XX**) - MAC address format to use for communication with RADIUS server

**radius-mac-mode** (*as-username | as-username-and-password*; default: **as-username**) - whether to use MAC address as username only or ad both username and password for RADIUS authentication

**static-algo-0** (*none | 40bit-wep | 104bit-wep | aes-ccm | tkip*; default: **none**) - which encryption algorithm to use:

- **none** - do not use encryption and do not accept encrypted packets
- **40bit-wep** - use the 40bit encryption (also known as 64bit-wep) and accept only these packets
- **104bit-wep** - use the 104bit encryption (also known as 128bit-wep) and accept only these packets
- **aes-ccm** - use the AES-CCM (Advanced Encryption Standard in Counter with CBC-MAC) encryption algorithm and accept only these packets
- **tkip** - use the TKIP (Temporal Key Integrity Protocol) and accept only these packets

**static-algo-1** (*none | 40bit-wep | 104bit-wep | aes-ccm | tkip*; default: **none**) - which encryption algorithm to use:

- **none** - do not use encryption and do not accept encrypted packets
- **40bit-wep** - use the 40bit encryption (also known as 64bit-wep) and accept only these packets
- **104bit-wep** - use the 104bit encryption (also known as 128bit-wep) and accept only these packets
- **aes-ccm** - use the AES-CCM (Advanced Encryption Standard in Counter with CBC-MAC) encryption algorithm and accept only these packets
- **tkip** - use the TKIP (Temporal Key Integrity Protocol) and accept only these packets

**static-algo-2** (*none* | *40bit-wep* | *104bit-wep* | *aes-ccm* | *tkip*; default: **none**) - which encryption algorithm to use:

- **none** - do not use encryption and do not accept encrypted packets
- **40bit-wep** - use the 40bit encryption (also known as 64bit-wep) and accept only these packets
- **104bit-wep** - use the 104bit encryption (also known as 128bit-wep) and accept only these packets
- **aes-ccm** - use the AES-CCM (Advanced Encryption Standard in Counter with CBC-MAC) encryption algorithm and accept only these packets
- **tkip** - use the TKIP (Temporal Key Integrity Protocol) and accept only these packets

**static-algo-3** (*none* | *40bit-wep* | *104bit-wep* | *aes-ccm* | *tkip*; default: **none**) - which encryption algorithm to use:

- **none** - do not use encryption and do not accept encrypted packets
- **40bit-wep** - use the 40bit encryption (also known as 64bit-wep) and accept only these packets
- **104bit-wep** - use the 104bit encryption (also known as 128bit-wep) and accept only these packets
- **aes-ccm** - use the AES-CCM (Advanced Encryption Standard in Counter with CBC-MAC) encryption algorithm and accept only these packets
- **tkip** - use the TKIP (Temporal Key Integrity Protocol) and accept only these packets

**static-key-0** (*text*) - hexadecimal key which will be used to encrypt packets with the 40bit-wep or 104bit-wep algorithm (algo-0). If AES-CCM is used, the key must consist of even number of characters and must be at least 32 characters long. For TKIP, the key must be at least 64 characters long and also must consist of even number characters

**static-key-1** (*text*) - hexadecimal key which will be used to encrypt packets with the 40bit-wep or 104bit-wep algorithm (algo-1). If AES-CCM is used, the key must consist of even number of characters and must be at least 32 characters long. For TKIP, the key must be at least 64 characters long and also must consist of even number characters

**static-key-2** (*text*) - hexadecimal key which will be used to encrypt packets with the 40bit-wep or 104bit-wep algorithm (algo-2). If AES-CCM is used, the key must consist of even number of characters and must be at least 32 characters long. For TKIP, the key must be at least 64 characters long and also must consist of even number characters

**static-key-3** (*text*) - hexadecimal key which will be used to encrypt packets with the 40bit-wep or 104bit-wep algorithm (algo-3). If AES-CCM is used, the key must consist of even number of characters and must be at least 32 characters long. For TKIP, the key must be at least 64 characters long and also must consist of even number characters

**static-sta-private-algo** (*none* | *40bit-wep* | *104bit-wep* | *aes-ccm* | *tkip*) - algorithm to use if the static-sta-private-key is set. Used to communicate between 2 devices

**static-sta-private-key** (*text*) - if this key is set in station mode, use this key for encryption. In AP mode you have to specify static-private keys in the access-list or use the Radius server using radius-mac-authentication. Used to communicate between 2 devices

**static-transmit-key** (*static-key-0* | *static-key-1* | *static-key-2* | *static-key-3*; default: **static-key-0**) - which key to use for broadcast packets. Used in AP mode

**supplicant-identity** (*text*; default: **MikroTik**) - EAP supplicant identity to use for RADIUS EAP authentication

**tls-certificate** (*name*) - select the certificate for this device from the list of imported certificates

**tls-mode** (*no-certificates* | *dont-verify-certificate* | *verify-certificate*; default: **no-certificates**) - TLS certificate mode

- **no-certificates** - certificates are negotiated dynamically using anonymous Diffie-Hellman MODP 2048 bit algorithm
- **dont-verify-certificate** - require a certificate, but do not check, if it has been signed by the available CA certificate
- **verify-certificate** - require a certificate and verify that it has been signed by the available CA certificate

**unicast-ciphers** (*multiple choice: tkip* | *aes-ccm*) - a set of ciphers used to encrypt frames sent to individual wireless station (unicast transfers) in the order of preference

- **tkip** - Temporal Key Integrity Protocol - encryption protocol, compatible with legacy WEP equipment, but enhanced to correct some of WEP flaws
- **aes-ccm** - more secure WPA encryption protocol, based on the reliable AES (Advanced Encryption Standard). Networks free of WEP legacy should use only this

**wpa-pre-shared-key** (*text*; default: `''`) - string, which is used as the WPA Pre Shared Key. It must be the same on AP and station to communicate

**wpa2-pre-shared-key** (*text*; default: `''`) - string, which is used as the WPA2 Pre Shared Key. It must be the same on AP and station to communicate

## Notes

The keys used for encryption are in hexadecimal form. If you use **40bit-wep**, the key has to be 10 characters long, if you use **104bit-wep**, the key has to be 26 characters long.

Prism card doesn't report that the use of WEP is required for all data type frames, which means that some clients will not see that access point uses encryption and will not be able to connect to such AP. This is a Prism hardware problem and can not be fixed. Use Atheros-based cards (instead of Prism) on APs if you want to provide WEP in your wireless network.

Wireless encryption cannot work together with wireless compression.

## Sniffer

Home menu level: */interface wireless sniffer*

## Description

With wireless sniffer you can sniff packets from wireless networks.

## Property Description

**channel-time** (*time*; default: **200ms**) - how long to sniff each channel, if multiple-channels is set to yes

**file-limit** (*integer*; default: **10**) - limits file-name's file size (measured in kilobytes)

**file-name** (*text*; default: **''**) - name of the file where to save packets in PCAP format. If file-name is not defined, packets are not saved into a file

**memory-limit** (*integer*; default: **1000**) - how much memory to use (in kilobytes) for sniffed packets

**multiple-channels** (yes | no; default: **no**) - whether to sniff multiple channels or a single channel

- **no** - wireless sniffer sniffs only one channel in frequency that is configured in /interface wireless
- **yes** - sniff in all channels that are listed in the scan-list in /interface wireless

**only-headers** (yes | no; default: **no**) - sniff only wireless packet headers

**receive-errors** (yes | no; default: **no**) - whether to receive packets with CRC errors

**streaming-enabled** (yes | no; default: **no**) - whether to send packets to server in TZSP format

**streaming-max-rate** (*integer*; default: **0**) - how many packets per second the router will accept

- **0** - no packet per second limitation

**streaming-server** (*IP address*; default: **0.0.0.0**) - streaming server's IP address

## Sniffer Sniff

Home menu level: */interface wireless sniffer sniff*

## Description

Wireless Sniffer Sniffs packets

## Property Description

**file-over-limit-packets** (*read-only: integer*) - how many packets are dropped because of exceeding file-limit

**file-saved-packets** (*read-only: integer*) - number of packets saved to file

**file-size** (*read-only: integer*) - current file size (kB)

**memory-over-limit-packets** (*read-only: integer*) - number of packets that are dropped because of exceeding memory-limit

**memory-saved-packets** (*read-only: integer*) - how many packets are stored in memory

**memory-size** (*read-only: integer*) - how much memory is currently used for sniffed packets (kB)

**processed-packets** (*read-only: integer*) - number of sniffed packets

**real-file-limit** (*read-only: integer*) - the real file size limit. It is calculated from the beginning of sniffing to reserve at least 1MB free space on the disk

**real-memory-limit** (*read-only: integer*) - the real memory size limit. It is calculated from the beginning of sniffing to reserve at least 1MB of free space in the memory

**stream-dropped-packets** (*read-only: integer*) - number of packets that are dropped because of exceeding streaming-max-rate

**stream-sent-packets** (*read-only: integer*) - number of packets that are sent to the streaming server

## Command Description

**save** - saves sniffed packets from the memory to file-name in PCAP format

## Sniffer Packets

### Description

Wireless Sniffer sniffed packets. If packets Cyclic Redundancy Check (CRC) field detects error, it will be displayed by crc-error flag.

### Property Description

**band** (*read-only: text*) - wireless band

**dst** (*read-only: MAC address*) - the receiver's MAC address

**freq** (*read-only: integer*) - frequency

**interface** (*read-only: text*) - wireless interface that captures packets

**signal@rate** (*read-only: text*) - at which signal-strength and rate was the packet received

**src** (*read-only: MAC address*) - the sender's MAC address

**time** (*read-only: time*) - time when the packet was received, starting from the beginning of sniffing

**type** (*read-only: assoc-req | assoc-req | reassoc-req | reassoc-req | probe-req | probe-req | beacon | atim | disassoc | auth | deauth | ps-poll | rts | cts | ack | cf-end | cf-endack | data | d-cfack | d-cfpoll | d-cfackpoll | data-null | nd-cfack | nd-cfpoll | nd-cfackpoll*) - type of the sniffed packet

### Example

Sniffed packets:

```
[admin@MikroTik] interface wireless sniffer packet> pr
Flags: E - crc-error
#   FREQ SIGNAL@RATE   SRC           DST           TYPE
0   2412 -73dBm@1Mbps    00:0B:6B:31:00:53 FF:FF:FF:FF:FF:FF beacon
1   2412 -91dBm@1Mbps    00:02:6F:01:CE:2E FF:FF:FF:FF:FF:FF beacon
2   2412 -45dBm@1Mbps    00:02:6F:05:68:D3 FF:FF:FF:FF:FF:FF beacon
3   2412 -72dBm@1Mbps    00:60:B3:8C:98:3F FF:FF:FF:FF:FF:FF beacon
4   2412 -65dBm@1Mbps    00:01:24:70:3D:4E FF:FF:FF:FF:FF:FF probe-req
5   2412 -60dBm@1Mbps    00:01:24:70:3D:4E FF:FF:FF:FF:FF:FF probe-req
6   2412 -61dBm@1Mbps    00:01:24:70:3D:4E FF:FF:FF:FF:FF:FF probe-req
```

## Snooper

Home menu level: */interface wireless snooper*

### Description

With wireless snoop you can monitor the traffic load on each channel.

## Property Description

**channel-time** (*time*; default: **200ms**) - how long to snoop each channel, if multiple-channels is set to yes

**multiple-channels** (yes | no; default: **no**) - whether to snoop multiple channels or a single channel

- **no** - wireless snoop snoops only one channel in frequency that is configured in /interface wireless
- **yes** - snoop in all channels that are listed in the scan-list in /interface wireless

**receive-errors** (yes | no; default: **no**) - whether to receive packets with CRC errors

## Command Description

**snoop** - starts monitoring wireless channels

- **wireless interface name** - interface that monitoring is performed on
- **BAND** - operating band

## Example

Snoop 802.11b network:

```
[admin@MikroTik] interface wireless snoop> snoop wlan1
BAND      FREQ      USE      BW      NET-COUNT STA-COUNT
2.4ghz-b  2412MHz   1.5%    11.8kbps 2         2
2.4ghz-b  2417MHz   1.3%    6.83kbps 0         1
2.4ghz-b  2422MHz   0.6%    4.38kbps 1         1
2.4ghz-b  2427MHz   0.6%    4.43kbps 0         0
2.4ghz-b  2432MHz   0.3%    2.22kbps 0         0
2.4ghz-b  2437MHz   0%      0bps     0         0
2.4ghz-b  2442MHz   1%      8.1kbps  0         0
2.4ghz-b  2447MHz   1%      8.22kbps 1         1
2.4ghz-b  2452MHz   1%      8.3kbps  0         0
2.4ghz-b  2457MHz   0%      0bps     0         0
2.4ghz-b  2462MHz   0%      0bps     0         0
[admin@MikroTik] interface wireless snoop>
```