

Wireless Client and Wireless Access Point Manual

Document revision 1.7 (Mon Oct 25 13:51:30 GMT 2004)
This document applies to Wandy RouterOS V2.8

Table of Contents

Table of Contents
General Information
Summary
Quick Setup Guide
Specifications
Related Documents
Description
Wireless Interface Configuration
Description
Property Description
Notes
Example
Nstreme Settings
Description
Property Description
Example
Nstreme2 Group Settings
Description
Property Description
Example
Registration Table
Description
Property Description
Example
Access List
Description
Property Description
Notes
Example
Info
Description
Property Description
Notes
Example
Virtual Access Point Interface

Description
Property Description
Notes
Example
WDS Interface Configuration
Description
Property Description
Notes
Example
Align
Description
Property Description
Notes
Example
Align Monitor
Description
Property Description
Example
Network Scan
Description
Property Description
Example
Wireless Security
Description
Property Description
Notes
Wireless Application Examples
AP to Client Configuration Example
WDS Configuration Example
Wireless Security Example
Troubleshooting
Description

General Information

Summary

The wireless interface operates using IEEE 802.11 set of standards. It uses radio waves as a physical signal carrier and is capable of wireless data transmission with speeds up to 108 Mbps (in 5GHz turbo-mode).

Wandy RouterOS supports the Intersil Prism II PC/PCI, Atheros AR5000, AR5001X,

AR5001X+, AR5002X+, and AR5004X+ chipset based wireless adapter 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](#)

Wandy RouterOS provides a complete support for IEEE 802.11a, 802.11b and 802.11g wireless networking standards. There are several features implemented for the wireless data communication in RouterOS - WEP (Wired Equivalent Privacy), AES encryption, WDS (Wireless Distribution System), DFS (Dynamic Frequency Selection), Alignment mode (for positioning antennas and monitoring wireless signal), VAP (Virtual Access Point), Fast Frames, disable packet forwarding among clients, and others. You can see the [feature list](#) which are supported by various cards.

The nstreme protocol is Wandy proprietary (i.e., incompatible with other vendors) wireless protocol created to improve point-to-point and point-to-multipoint wireless links. Nstreme2 works with a pair of wireless cards (Atheros AR5210, AR5211, AR5212 and AR5213 MAC chips only) - one for transmitting data and one for receiving.

Benefits of nstreme protocol:

- Client polling
- Very low protocol overhead per frame allowing super-high data rates
- No protocol limits on link distance
- No 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 in compatibility mode (i.e., both 802.11b and 802.11g clients are allowed to connect), using frequency **2442 MHz** and Service Set Identifier **test**:

```
/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**:

```
/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)*

Home menu level: */interface wireless*

Standards and Technologies: *IEEE802.11a, IEEE802.11b, IEEE802.11g*

Hardware usage: *Not significant*

Related Documents

- [Package Management](#)
- [Device Driver List](#)
- [IP Addresses and ARP](#)
- [Log Management](#)

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.

Nstreme has no distance limitations.

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 a **dynamic** value - the router will determine the **ack-timeout** setting automatically.

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 Wandy RouterOS supports as many Atheros chipset based cards as many free adapter slots are there 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. Via Epia, Wandy RouterBoard 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.

Wireless Interface Configuration

Home menu level: */interface wireless*

Description

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

Property Description

802.1x-mode (*PEAP-MSCHAPV2* | *none*; default: **no**) - whether to use Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol version 2 for Authentication

ack-timeout (*integer* | *dynamic* | *indoor*) - acknowledgment code timeout (transmission acceptance timeout) in microseconds or one of these:

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

antenna-mode (*ant-a* | *ant-b* | *rx-a-tx-b* | *tx-a-rx-b*; default: **ant-a**) - which antenna to use for transmit/receive data:

- **ant-a** - use only antenna a
- **ant-b** - use only antenna b
- **rx-a-tx-b** - use antenna a for receiving packets, use antenna b for transmitting packets
- **tx-a-rx-b** - use antenna a for transmitting packets, antenna b for receiving packets

arp - Address Resolution Protocol setting

band - operating band

- **2.4ghz-b** - IEEE 802.11b
- **2.4ghz-b/g** - IEEE 802.11b and IEEE 802.11g
- **2.4ghz-g-turbo** - IEEE 802.11g up to 108 Mbit
- **2.4ghz-onlyg** - IEEE 802.11g
- **5ghz** - IEEE 802.11a up to 54 Mbit
- **5ghz-turbo** - IEEE 802.11a up to 108Mbit

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). 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). 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 other wireless cards in that network will not be able to transmit data for burst-time microseconds. This setting is available only for AR5000, AR5001X, and AR5001X+ chipset based cards

default-authentication (yes | no; default: **yes**) - specifies the default action for clients or APs that are not in access list

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

default-forwarding (yes | no; default: **yes**) - 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 while working in AP mode, the AP continues searching for the next available channel where no radar is 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

fast-frames (*yes | no*; default: **no**) - whether to pack smaller packets into a larger one, which makes larger data rates possible

frequency (*integer*; default: **5120**) - operating frequency of the card

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
ant to 'broadcast ssid' (empty ssid)

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

mac-address (*read-only: MAC address*) - MAC address

master-device (*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

mode (*alignment-only | ap-bridge | bridge | nstreme-dual-slave | station | 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
- **nstreme-dual-slave** - the interface is used for nstreme-dual mode
- **station** - the interface is operating as a client
- **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**) - value in dBm below which we say that it is rather noise than a normal signal

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

radio-name (*name*) - MT proprietary extension for Atheros cards

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-ism*; default: **default-ism**) - the list of channels to scan

- **default-ism** - for 2.4ghz mode: 2412, 2417, 2422, 2427, 2432, 2437, 2442, 2447, 2452, 2457, 2462, 2467, 2472; for 5ghz mode: 5180, 5200, 5220, 5240, 5260, 5280, 5300, 5320, 5745, 5765, 5785, 5805; for 5ghz-turbo: 5210, 5250, 5290, 5760, 5800

server-certificate - not implemented, yet

ssid (*text*; default: **Wandy**) - 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* | *default*; default: **default**) - transmit power in dB

- **default** - default value of the card

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-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

Notes

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

Before it will be possible to manually control

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.

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**. You should set **tx-power** property to an appropriate value as many cards do not have their default setting set to the maximal power it can work on. For the cards Wandy is selling (5G/ABM), 20dB (100mW) is the maximal power in 5GHz bands and 18dB (65mW) is the maximal power in 2.4GHz bands.

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 wireless interfaces are put in **nstreme-dual-slave** mode, all configuration will take place in **/interface wireless nstreme-dual** submenu described further on. In that case, configuration made in this submenu will be ignored.

Example

Let us consider an example: a Wandy router is connected to an AP using Atheros card and the AP is operating in IEEE 802.11b standard with **ssid=hotspot**.

To see current interface settings:

```
[admin@Wandy] interface wireless> print
Flags: X - disabled, R - running
0 X name="wlan1" mtu=1500 mac-address=00:01:24:70:3D:4E arp=enabled
disable-running-check=no interface-type=Atheros AR5211 mode=station
ssid="Wandy" frequency=5180 band=5GHz scan-list=default-ism
supported-rates-b=1Mbps,2Mbps,5.5Mbps,11Mbps
supported-rates-a/g=6Mbps,9Mbps,12Mbps,18Mbps,24Mbps,36Mbps,48Mbps,
54Mbps

basic-rates-b=1Mbps basic-rates-a/g=6Mbps max-station-count=2007
ack-timeout=dynamic tx-power=default noise-floor-threshold=default
burst-time=disabled fast-frames=no dfs-mode=none antenna-mode=ant-a
wds-mode=disabled wds-default-bridge=none wds-ignore-ssid=no
default-authentication=yes default-forwarding=yes hide-ssid=no
802.1x-mode=none

[admin@Wandy] interface wireless>
```

Set the **ssid** to *hotspot* and enable the interface. Use the monitor command to see the connection status.

```
[admin@Wandy] interface wireless> set 0 ssid=hotspot band=2.4ghz-b \
disabled=no
[admin@Wandy] interface wireless> mo 0
status: connected-to-ess
band: 2.4ghz-b
frequency: 2442
tx-rate: 11Mbps
rx-rate: 11Mbps
ssid: hotspot
bssid: 00:0B:6B:31:08:22
```

```
radio-name: 000B6B310822
signal-strength: -55
tx-signal-strength: -55
tx-ccq: 99
rx-ccq: 98
current-ack-timeout: 110
current-distance: 110
wds-link: no
nstreme: no
framing-mode: none
routeros-version: 2.8.15
last-ip: 192.168.0.254
```

```
[admin@Wandy] interface wireless>
```

Monitor from the Access Point:

```
[admin@AP] interface wireless> mo 0
status: running-ap
band: 2.4ghz-b
frequency: 2442
overall-tx-ccq: 58
registered-clients: 2
current-ack-timeout: 30
current-distance: 30
nstreme: no
```

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

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* | *fast-frames* | *dynamic-size*; default: **none**) - the method how to combine frames (like fast-frames setting in interface configuration). A number of frames

may be combined into one bigger one to reduce the amount of protocol overhead (and thus increase

speed). The card are not waiting for frames, but in case a number packets are queued for transmitting, they can be combined. There are several methods of framing:

- **none** - do nothing special, do not combine packets
- **fast-frames** - use fast-frame mode of the radio card
- **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

Example

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

```
[admin@Wandy] interface wireless nstreme> print
0 name="wlan1" enable-nstreme=no enable-polling=yes framer-policy=none
framer-limit=3200
[admin@Wandy] 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

Property Description

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

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: **4000**) - maximal frame size

framer-policy (*none | best-fit | exact-size*; default: **none**) - the method how to combine frames (like fast-frames setting in interface configuration). A number of frames may be combined into one

bigger one to reduce the amount of protocol overhead (and thus increase speed). The card are not

waiting for frames, but in case a number 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 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)

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

mtu (*integer: 0..65536*; 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)

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)

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

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

Example

To enable the nstreme2 protocol on a router:

1. Having two Atheros AR5212 based cards which are not used for anything else, to group them into a nstreme interface, switch both of them into **nstreme-slave** mode:

```
[admin@Wandy] interface wireless> print
Flags: X - disabled, R - running
0 name="wlan1" mtu=1500 mac-address=00:0B:6B:31:02:4F arp=enabled
disable-running-check=no interface-type=Atheros AR5212
radio-name="000B6B31024F" mode=station ssid="Wandy" frequency=5180
band=5GHz scan-list=default-ism
supported-rates-b=1Mbps,2Mbps,5.5Mbps,11Mbps
supported-rates-a/g=6Mbps,9Mbps,12Mbps,18Mbps,24Mbps,36Mbps,48Mbps,
54Mbps
basic-rates-b=1Mbps basic-rates-a/g=6Mbps max-station-count=2007
ack-timeout=dynamic tx-power=default noise-floor-threshold=default
burst-time=disabled fast-frames=no dfs-mode=disabled antenna-mode=ant-a
wds-mode=disabled wds-default-bridge=none
update-stats-interval=disabled default-authentication=yes
default-forwarding=yes hide-ssid=no 802.1x-mode=none

1 name="wlan2" mtu=1500 mac-address=00:0B:6B:30:B4:A4 arp=enabled
disable-running-check=no interface-type=Atheros AR5212
radio-name="000B6B30B4A4" mode=station ssid="Wandy" frequency=5180
band=5GHz scan-list=default-ism
supported-rates-b=1Mbps,2Mbps,5.5Mbps,11Mbps
supported-rates-a/g=6Mbps,9Mbps,12Mbps,18Mbps,24Mbps,36Mbps,48Mbps,
54Mbps
basic-rates-b=1Mbps basic-rates-a/g=6Mbps max-station-count=2007
ack-timeout=dynamic tx-power=default noise-floor-threshold=default
burst-time=disabled fast-frames=no dfs-mode=none antenna-mode=ant-a
wds-mode=disabled wds-default-bridge=none
update-stats-interval=disabled default-authentication=yes
default-forwarding=yes hide-ssid=no 802.1x-mode=none

[admin@Wandy] interface wireless> set 0,1 mode=nstreme-dual-slave
```

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

```
[admin@Wandy] interface wireless nstreme-dual> add \
```

```
\... framer-policy=exact-size
```

3. And configure which card will be receiving, and which - transmitting

```
[admin@Wandy] interface wireless nstreme-dual> print
Flags: X - disabled, R - running
0 X name="n-streme1" 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
rates-b=1Mbps,2Mbps,5.5Mbps,11Mbps
rates-a/g=6Mbps,9Mbps,12Mbps,18Mbps,24Mbps,36Mbps,48Mbps,54Mbps
rx-band=5GHz rx-frequency=5320 framer-policy=exact-size
framer-limit=4000
```

```
[admin@Wandy] interface wireless nstreme-dual> set 0 disabled=no \
\... tx-radio=wlan1 rx-radio=wlan2
[admin@Wandy] 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

ack-timeout (*read-only: integer*) - acknowledgment code timeout (transmission acceptance timeout) in microseconds or one of these

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

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

distance (*read-only: integer*) - the same as ack-timeout

framing-mode (*read-only: none | best-fit | exact-size | fast-frames | dynamic-size*; default: **none**) - the method how the frames are combined

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

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

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

nstreme (*read-only: yes | no*) - whether the client uses Nstreme protocol or not

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

radio-name (*read-only: name*) - MT proprietary extension for Atheros cards

routeros-version (*read-only: text*) - if the client is a Wandy router, this value shows its version

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

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

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

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

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

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

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

wds (*read-only: yes | no*) - whether client uses WDS or not

Example

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

```
[admin@Wandy] interface wireless registration-table> print
# INTERFACE RADIO-NAME MAC-ADDRESS AP SIGNAL... TX-RATE
0 wlan1 000124703D61 00:01:24:70:3D:61 no -66 9Mbps
```

To get additional statistics:

```
[admin@Wandy] interface wireless> registration-table print stats
0 interface=wlan1 radio-name="000124703D61" mac-address=00:01:24:70:3D:61
ap=no wds=no rx-rate=54Mbps tx-rate=9Mbps packets=4,28 bytes=41,2131
frames=4,28 frame-bytes=41,2131 hw-frames=4,92 hw-frame-bytes=137,4487
uptime=00:11:08 last-activity=00:00:03.940 signal-strength=-66
```

```
tx-signal-strength=-61 tx-ccq=2 rx-ccq=1 ack-timeout=28 distance=28
nstreme=no framing-mode=none routers-version="2.8.14"
[admin@Wandy] interface wireless>
```

Access List

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

Description

The access list is used by the Access Point to restrict associations of clients and by clients to restrict associations to a given list of APs. This list contains MAC address of client and associated action to take when client attempts to connect. Also, the forwarding of frames sent by the client is controlled.

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 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

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

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

interface (*name*) - AP interface name

mac-address (*MAC address*) - MAC address of the client

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

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

skip-802.1x (yes | no) - not implemented, yet

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@Wandy] interface wireless access-list> add mac-address= \
\... 00:01:24:70:3A:BB interface=wlan1 private-algo=40bit-wep private-
key=1234567890
[admin@Wandy] interface wireless access-list> print
Flags: X - disabled
0 mac-address=00:01:24:70:3A:BB interface=wlan1 authentication=yes
forwarding=yes skip-802.1x=yes private-algo=40bit-wep
private-key="1234567890"
[admin@Wandy] 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 2.4ghz 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 2.4ghz 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,*

Page 14 of 28

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)

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

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

supported-bands (*multiple choice, read-only: 2ghz-b | 2ghz-g | 5ghz | 5ghz-turbo*) - 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.

In RouterOS v2.8 and above **/interface wireless info print** command shows only channels supported by particular card. This behaviour differs from one in v2.7, where **wireless info print** command showed all channels, even those not supported by particular card.

Example

```
[admin@Wandy] interface wireless info> print
0 interface-type=Atheros AR5212 tx-power-control=yes ack-timeout-control=yes
alignment-mode=yes virtual-aps=yes noise-floor-control=yes
scan-support=yes burst-support=yes nstreme-support=yes
supported-bands=2ghz-b,5ghz,5ghz-turbo,2ghz-g
2ghz-b-channels=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
5ghz-channels=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
5ghz-turbo-channels=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
2ghz-g-channels=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
[admin@Wandy] interface wireless info>

```

Virtual Access Point Interface

Home menu level: */interface wireless*

Description

Virtual Access Point (VAP) interface is used to have an additional AP. You can create a new AP with different **ssid**. It can be compared with a VLAN where the **ssid** from VAP is the **VLAN tag** and the hardware interface is the VLAN switch.

Note that you cannot use the Virtual Access Point on Prism based cards!

Property Description

802.1x-mode (*PEAP-MSCHAPV2* | *none*) - to use Protected Extensible Authentication Protocol
Microsoft Challenge Handshake Authentication Protocol version 2 for authentication

arp (*disabled* | *enabled* | *proxy-arp* | *reply-only*) - ARP mode

default-authentication (*yes* | *no*; default: **yes**) - whether to accept or reject a client that wants to associate, but is not in the access-list

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

disabled (*yes* | *no*; default: **yes**) - whether to disable the interface 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'

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 (*read-only: MAC address*; default: **00:00:00:00:00:00**) - MAC address of VAP. Is assigned automatically when the field master interface is set

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

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

Notes

You can create a VAP only in the same frequency and the same band as specified in the **master-interface**

Example

Add a VAP:

```
/interface wireless add master-interface=wlan1 ssid=VAP1 disabled=no
[admin@Wandy] interface wireless> print
Flags: X - disabled, R - running
0 R name="wlan1" mtu=1500 mac-address=00:0B:6B:31:02:4B arp=enabled
disable-running-check=no interface-type=Atheros AR5212
radio-name="AP_172" mode=ap-bridge ssid="wtest" frequency=5805
band=5ghz scan-list=default-ism rate-set=default
supported-rates-b=1Mbps,2Mbps,5.5Mbps,11Mbps
supported-rates-a/g=6Mbps,9Mbps,12Mbps,18Mbps,24Mbps,36Mbps,48Mbps,
54Mbps
basic-rates-b=1Mbps basic-rates-a/g=6Mbps max-station-count=2007
ack-timeout=dynamic tx-power=default noise-floor-threshold=default
burst-time=disabled fast-frames=no dfs-mode=none antenna-mode=ant-a
wds-mode=disabled wds-default-bridge=none wds-ignore-ssid=no
update-stats-interval=disabled default-authentication=yes
default-forwarding=yes hide-ssid=no 802.1x-mode=none
1 name="wlan2" mtu=1500 mac-address=00:0B:6B:31:02:4B arp=enabled
disable-running-check=no interface-type=virtual-AP
master-interface=wlan1 ssid="VAP1" max-station-count=2007
default-authentication=yes default-forwarding=yes hide-ssid=no
802.1x-mode=none
[admin@Wandy] interface wireless>
```

Now you can connect clients to 8AP with **ssid=VAP1**

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 (*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..65336*; 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.

Example

```
[admin@Wandy] interface wireless wds> add master-interface=wlan1 \  
\... wds-address=00:0B:6B:30:2B:27 disabled=no  
[admin@Wandy] 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@Wandy] 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: **64**) - signal-strength at which audio (beeper) frequency will be the highest

audio-min (*integer*; default: **0**) - 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

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@Wandy] 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: 0
audio-max: 64
[admin@Wandy] 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

Page 20 of 28

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

Example

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

Network Scan

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

(name) - interface name to use for scanning

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

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

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

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

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

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

Example

```
[admin@Wandy] interface wireless> scan wlan1 refresh-interval=1s
# ADDRESS SSID BAND FREQ BSS PRIVACY SIGNAL-STRENGTH
0 00:02:6F:01:69:FA wep2 2.4GHz-B 2412 yes no -59
0 00:02:6F:20:28:E6 r 2.4GHz-B 2422 yes no -79
0 00:02:6F:05:68:D3 hotspot 2.4GHz-B 2442 yes no -95
0 00:40:96:44:2E:16 2.4GHz-B 2457 yes no -84
0 00:02:6F:08:53:1F rbininstall 2.4GHz-B 2457 yes no -93

[admin@Wandy] interface wireless>
```

Wireless Security

Description

This section provides the WEP (Wired Equivalent Privacy) functions to wireless interfaces.

Property Description

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

- **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 (Advanced Encryption Standard) with CCM (Counter with CBC-MAC) encryption and accept only these packets
- **none** - do not use encryption and do not accept encrypted packets

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

- **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 (Advanced Encryption Standard) with CCM (Counter with CBC-MAC) encryption and accept only these packets
- **none** - do not use encryption and do not accept encrypted packets

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

- **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 (Advanced Encryption Standard) with CCM (Counter with CBC-MAC) encryption and accept only these packets
- **none** - do not use encryption and do not accept encrypted packets

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

- **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 (Advanced Encryption Standard) with CCM (Counter with CBC-MAC)

encryption and accept only these packets

- **none** - do not use encryption and do not accept encrypted packets

key-0 (*text*) - hexadecimal key which will be used to encrypt packets with the 40bit-wep, 104bit-wep or aes-ccm algorithm (algo-0)

key-1 (*text*) - hexadecimal key which will be used to encrypt packets with the 40bit-wep, 104bit-wep or aes-ccm algorithm (algo-0)

key-2 (*text*) - hexadecimal key which will be used to encrypt packets with the 40bit-wep, 104bit-wep or aes-ccm algorithm (algo-0)

key-3 (*text*) - hexadecimal key which will be used to encrypt packets with the 40bit-wep, 104bit-wep or aes-ccm algorithm (algo-0)

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

security (*none | optional | required*; default: **none**) - security level:

- **none** - do not encrypt packets and do not accept encrypted packets

- **optional** - if there is a sta-private-key set, use it. Otherwise, if the ap-bridge mode is set - do not

use encryption, if the mode is station, use encryption if the transmit-key is set

- **required** - encrypt all packets and accept only encrypted packets

sta-private-algo (*40bit-wep | 104bit-wep | aes-ccm | none*) - algorithm to use if the sta-private-key

is set. Used to communicate between 2 devices

sta-private-key (*text*) - if this key is set in station mode, use this key for encryption. In ap-bridge

mode you have to specify private keys in the access-list or use the Radius server using radius-mac-authentication. Used to communicate between 2 devices

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

Used in AP mode

Notes

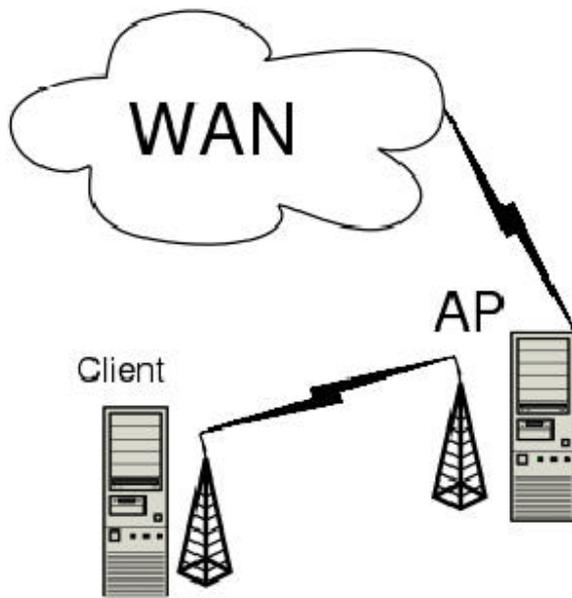
The keys used for encryption are in hexadecimal form. If you use **40bit-wep**, the key has to be 10

characters long, if you use **104bit-wep**, the key has to be 26 characters long, **aes-ccm** key should

contain 32 hexadecimal characters.

Application Examples

AP to Client Configuration Example



You need Level5 license to enable the AP mode. To make the Wandy router to work as an access point, the configuration of the wireless interface should be as follows:

- A unique Service Set Identifier should be chosen, say "test1"
- A frequency should be selected for the link, say 5180MHz
- The operation mode should be set to **ap-bridge**

The following command should be issued to change the settings for the wireless AP interface:

```
[admin@AP] interface wireless> set 0 mode=ap-bridge ssid=test1 \  
\... disabled=no frequency= 5180 band=5GHz  
[admin@AP] interface wireless> print  
Flags: X - disabled, R - running  
0 name="wlan1" mtu=1500 mac-address=00:0B:6B:31:01:6A arp=enabled  
disable-running-check=no interface-type=Atheros AR5212 mode=ap-bridge  
ssid="test1" frequency=5180 band=5GHz scan-list=default-ism
```

```

supported-rates-b=1Mbps,2Mbps,5.5Mbps,11Mbps
supported-rates-a/g=6Mbps,9Mbps,12Mbps,18Mbps,24Mbps,36Mbps,48Mbps,
54Mbps
basic-rates-b=1Mbps basic-rates-a/g=6Mbps max-station-count=2007
ack-timeout=dynamic tx-power=default noise-floor-threshold=default
burst-time=disabled fast-frames=no antenna-mode=ant-a wds-mode=disabled
wds-default-bridge=none default-authentication=yes
default-forwarding=yes hide-ssid=no 802.1x-mode=none

[admin@AP] interface wireless>

```

Then we need to configure the wireless client interface:

```

[admin@Wandy] interface wireless> set 0 mode=station ssid=test1 \
\... disabled=no
[admin@Client] interface wireless> print
Flags: X - disabled, R - running
0 R name="wlan2" mtu=1500 mac-address=00:0B:6B:30:79:02 arp=enabled
disable-running-check=no interface-type=Atheros AR5212 mode=station
ssid="test1" frequency=5180 band=5GHz scan-list=default-ism
supported-rates-b=1Mbps,2Mbps,5.5Mbps,11Mbps
supported-rates-a/g=6Mbps,9Mbps,12Mbps,18Mbps,24Mbps,36Mbps,48Mbps,
54Mbps
basic-rates-b=1Mbps basic-rates-a/g=6Mbps max-station-count=2007
ack-timeout=dynamic tx-power=default noise-floor-threshold=default
burst-time=disabled fast-frames=no antenna-mode=ant-a wds-mode=disabled
wds-default-bridge=none default-authentication=yes
default-forwarding=yes hide-ssid=no 802.1x-mode=none

[admin@Client] interface wireless>

```

Now we can monitor our connection from the AP:

```

[admin@AP] interface wireless> monitor 0
status: running-ap
registered-clients: 1
current-ack-timeout: 28
current-distance: 28

[admin@AP] interface wireless>

```

... and from the client:

```

[admin@Client] interface wireless> monitor 0
status: connected-to-ess
band: 5GHz
frequency: 5180
tx-rate: 6Mbps
rx-rate: 6Mbps
ssid: test1
bssid: 00:0B:6B:31:01:6A
signal-strength: -66
current-ack-timeout: 28
current-distance: 28

[admin@Client] interface wireless>

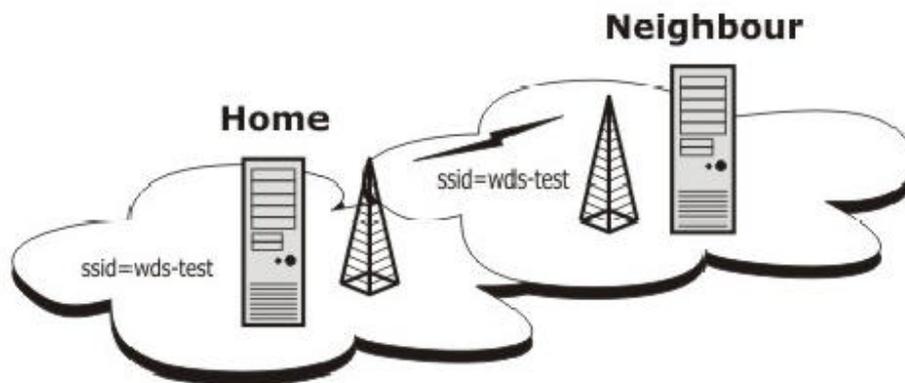
```

WDS Configuration Example

WDS (Wireless Distribution System) makes it able to connect APs to each other with the same **ssid** and share the same network. On one physical wireless interface you can create multiple WDS interfaces which will connect to other APs.

This is just a simple example how to get a connection between APs using WDS. Afterwards you can bridge it with the wireless and/or ethernet interface.

Let us consider the following example:



Router **Home**

- ssid = wds-test
- IP Address = 192.168.0.2
- Network Mask = 255.255.255.0

Router **Neighbour**

- ssid = wds-test
- IP Address = 192.168.0.1
- Network Mask = 255.255.255.0

Router **Home** configuration.

At first we should configure the wireless interface for router **Home**:

```
[admin@Home] interface wireless> set wlan1 mode=ap-bridge ssid=wds-test \  
\... wds-mode=static disabled=no  
[admin@Home] interface wireless> print  
Flags: X - disabled, R - running  
0 name="wlan1" mtu=1500 mac-address=00:01:24:70:3A:83 arp-enabled  
disable-running-check=no interface-type=Atheros AR5211 mode=ap-bridge  
Page 25 of 28  
ssid="wds-test" frequency=5120 band=5GHz scan-list=default-ism
```

```
supported-rates-a/g=6Mbps,9Mbps,12Mbps,18Mbps,24Mbps,36Mbps,48Mbps,54Mbps
basic-rates-a/g=6Mbps supported-rates-b=1Mbps,2Mbps,5.5Mbps,11Mbps
basic-rates-b=1Mbps max-station-count=2007 ack-timeout=default
tx-power=default noise-floor-threshold=default wds-mode=static
wds-default-bridge=none default-authentication=yes
default-forwarding=yes hide-ssid=no 802.1x-mode=none
```

```
[admin@Home] interface wireless>
```

We should add and configure a **WDS** interface. Note that the value of **wds-address** is the remote

wds host's wireless interface MAC address (to which we will connect to):

```
[admin@Home] interface wireless wds> add wds-address=00:01:24:70:3B:AE \
\... master-inteface=wlan1 disabled=no
[admin@Home] interface wireless wds> print
Flags: X - disabled, R - running, D - dynamic
0 name="wds1" mtu=1500 mac-address=00:01:24:70:3A:83 arp=enabled
disable-running-check=no master-inteface=wlan1
wds-address=00:01:24:70:3B:AE
```

```
[admin@Home] interface wireless wds>
```

Add the IP address to the **WDS** interface:

```
[admin@Home] ip address> add address=192.168.25.2/24 interface=wds1
[admin@Home] ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK BROADCAST INTERFACE
0 192.168.25.2/24 192.168.25.0 192.168.25.255 wds1
```

```
[admin@Home] ip address>
```

Router Neighbour configuration.

At first we should configure the wireless interface for router **Neighbour**:

```
[admin@Neighbour] interface wireless> set wlan1 mode=ap-bridge ssid=wds-test \
\... wds-mode=static disabled=no
[admin@Neighbour] interface wireless> print
Flags: X - disabled, R - running
0 R name="wlan1" mtu=1500 mac-address=00:01:24:70:3B:AE arp=enabled
disable-running-check=no interface-type=Atheros AR5211 mode=ap-bridge
ssid="wds-test" frequency=5120 band=5GHz scan-list=default-ism
supported-rates-a/g=6Mbps,9Mbps,12Mbps,18Mbps,24Mbps,36Mbps,48Mbps,54Mbps
basic-rates-a/g=6Mbps supported-rates-b=1Mbps,2Mbps,5.5Mbps,11Mbps
basic-rates-b=1Mbps max-station-count=2007 ack-timeout=default
tx-power=default noise-floor-threshold=default wds-mode=static
wds-default-bridge=none default-authentication=yes
default-forwarding=yes hide-ssid=no 802.1x-mode=none
```

```
[admin@Neighbour] interface wireless>
```

Now the **WDS** interface configuration:

```
[admin@Neighbour] interface wireless wds> add wds-address=00:01:24:70:3A:83 \
\... master-inteface=wlan1 disabled=no
```

```
[admin@Neighbour] interface wireless wds> print
Flags: X - disabled, R - running, D - dynamic
0 R name="wds1" mtu=1500 mac-address=00:01:24:70:3B:AE arp=enabled
disable-running-check=no master-inteface=wlan1
wds-address=00:01:24:70:3A:83
```

```
[admin@Neighbour] interface wireless wds>
```

Add the IP address:

```
[admin@Neighbour] ip address> add address=192.168.25.1/24 interface=wds1
[admin@Neighbour] ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK BROADCAST INTERFACE
0 192.168.25.1/24 192.168.25.0 192.168.25.255 wds1

[admin@Neighbour] ip address>
```

And now you can check whether the **WDS** link works:

```
[admin@Neighbour] ip address> /ping 192.168.25.2
192.168.25.2 64 byte ping: ttl=64 time=6 ms
192.168.25.2 64 byte ping: ttl=64 time=4 ms
192.168.25.2 64 byte ping: ttl=64 time=4 ms
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4/4.4/6 ms

[admin@Neighbour] ip address>
```

Wireless Security Example

Let us consider that we want to secure all data for all wireless clients that are connecting to our AP.

At first, add addresses to the wireless interfaces.

On the AP:

```
[admin@AP] ip address> add address=192.168.1.1/24 interface=wlan1
[admin@AP] ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK BROADCAST INTERFACE
0 192.168.1.1/24 192.168.1.0 192.168.1.255 wlan1

[admin@AP] ip address>
```

And on the client:

```
[admin@Client] ip address> add address=192.168.1.2/24 interface=wlan1
[admin@AP] ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK BROADCAST INTERFACE
0 192.168.1.2/24 192.168.1.0 192.168.1.255 wlan1
[admin@Client] ip address>
```

On the AP set the security to **required** and choose which encryption algorithm to use:

```
[admin@AP] interface wireless security> set 0 security=required \
\... algo-1=40bit-wep key-1=0123456789 transmit-key=key-1
[admin@AP] interface wireless security> print
0 name="wlan1" security=required algo-0=none key-0=""
algo-1=40bit-wep key-1="0123456789" algo-2=none key-2="" algo-3=none key-3=""
transmit-key=key-1 sta-private-algo=none sta-private-key=""
radius-mac-authentication=no
[admin@AP] interface wireless security>
```

On the client side do the same:

```
[admin@Client] interface wireless security> set 0 security=required \
\ algo-1=40bit-wep key-1=0123456789 transmit-key=key-1
[admin@AP] interface wireless security> print
0 name="wlan1" security=required algo-0=none key-0=""
algo-1=40bit-wep key-1="0123456789" algo-2=none key-2="" algo-3=none key-3=""
transmit-key=key-1 sta-private-algo=none sta-private-key=""
radius-mac-authentication=no
[admin@Client] interface wireless security>
```

Finally, test the link:

```
[admin@Client] interface wireless security> /ping 192.168.1.1
192.168.1.1 64 byte ping: ttl=64 time=22 ms
192.168.1.1 64 byte ping: ttl=64 time=16 ms
192.168.1.1 64 byte ping: ttl=64 time=15 ms
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 15/17.6/22 ms

[admin@Client] interface wireless security>
```

Troubleshooting

Description

- **If I use WDS and DFS, the routers do not connect to each other!**

As the WDS routers must operate at the same frequency, it is very probable that DFS will not select the frequency that is used by the peer router.

- **Wandy RouterOS does not send any traffic through Cisco Wireless Access Point or Wireless Bridge**

If you use CISCO/Aironet Wireless Ethernet Bridge or Access Point, you should set the Configuration/Radio/I80211/Extended (Allow proprietary extensions) to **off**, and the Configuration/Radio/I80211/Extended/Encapsulation (Default encapsulation method) to **RFC1042**. If left to the default **on** and **802.1H**, respectively, you won't be able to pass traffic through the bridge.