

Wireless Workshop

MUM 2012 - Warsaw

Uldis Cernevskis

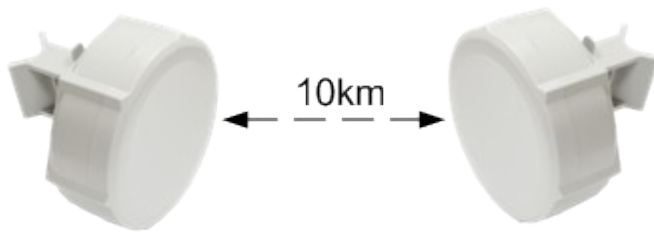
MikroTik

Topics

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

Connection Types

Point to Point (PTP)



Point to Multi Point (PTMP)



PTP/PTMP connection modes

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

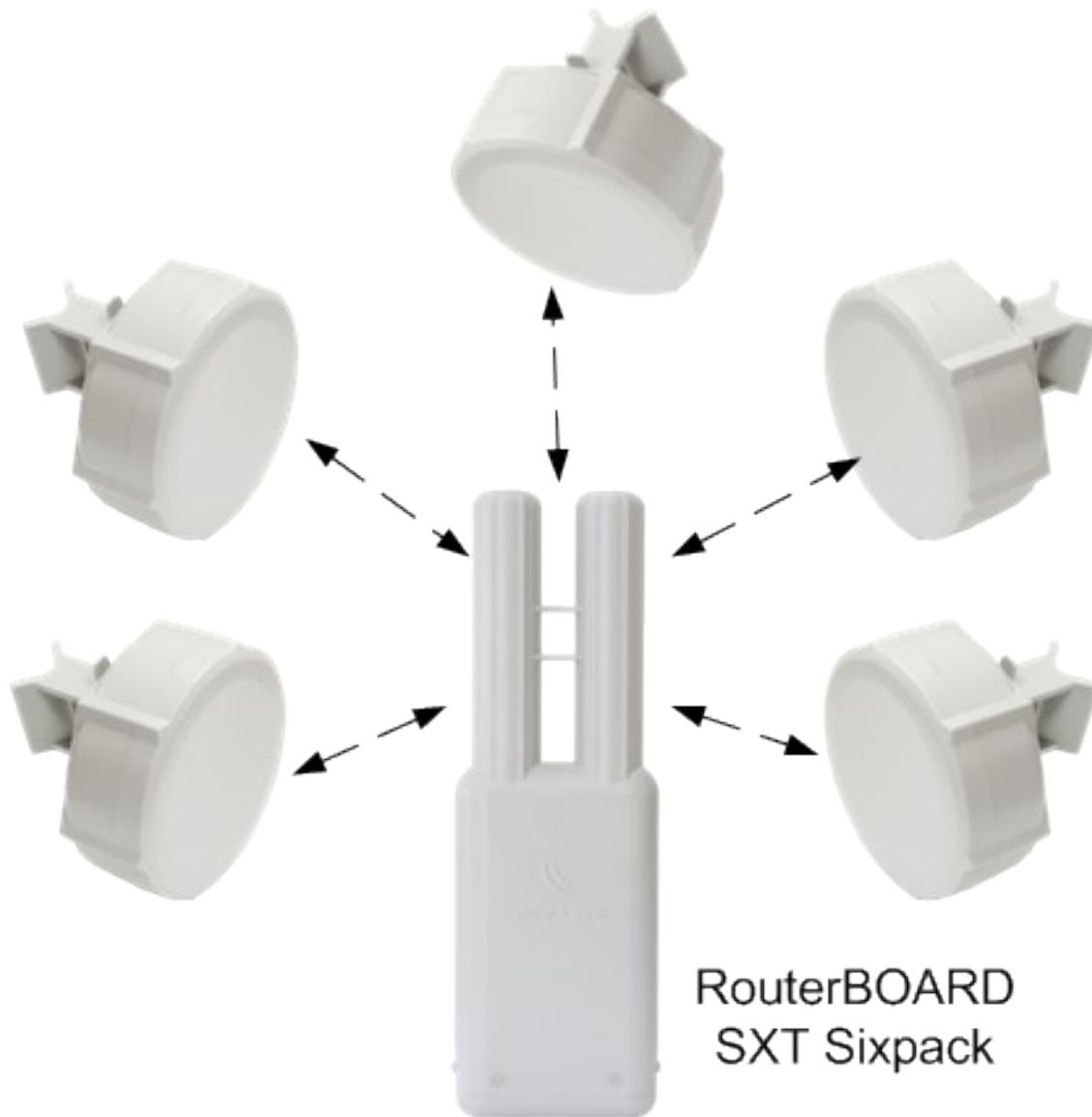
RouterOS license requirements

- PTP link requires at least Level 3
 - Example: Bridge <-> Station
- PTMP link requires on AP at least Level 4 and on clients at least Level 3
 - Example: AP-bridge <-> Station

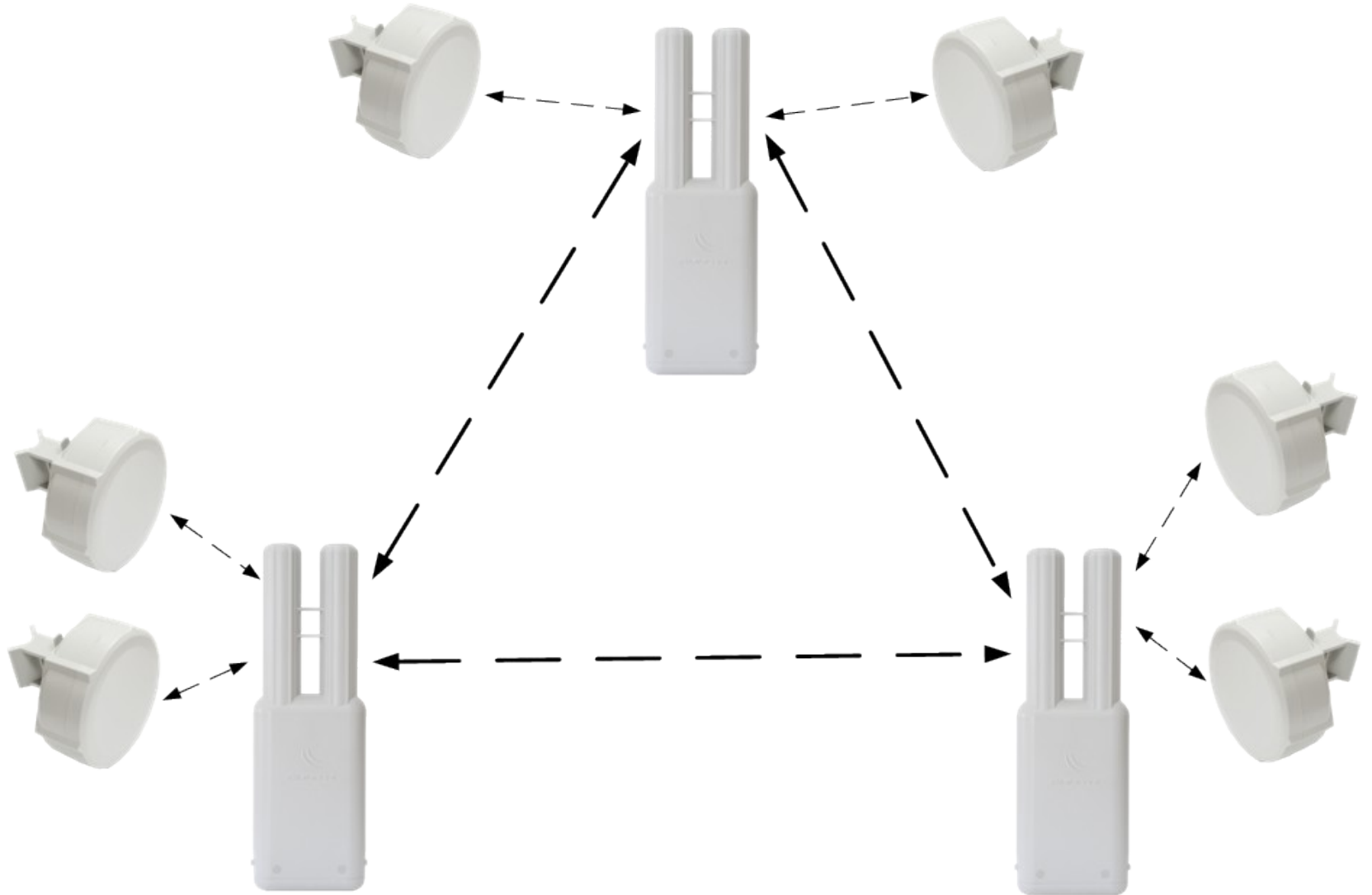
Wireless Standards and Protocols

- RouterOS PTP and PTMP supports
 - 802.11 a/b/g/n standards
 - 802.11, Nstreme and Nv2 protocols

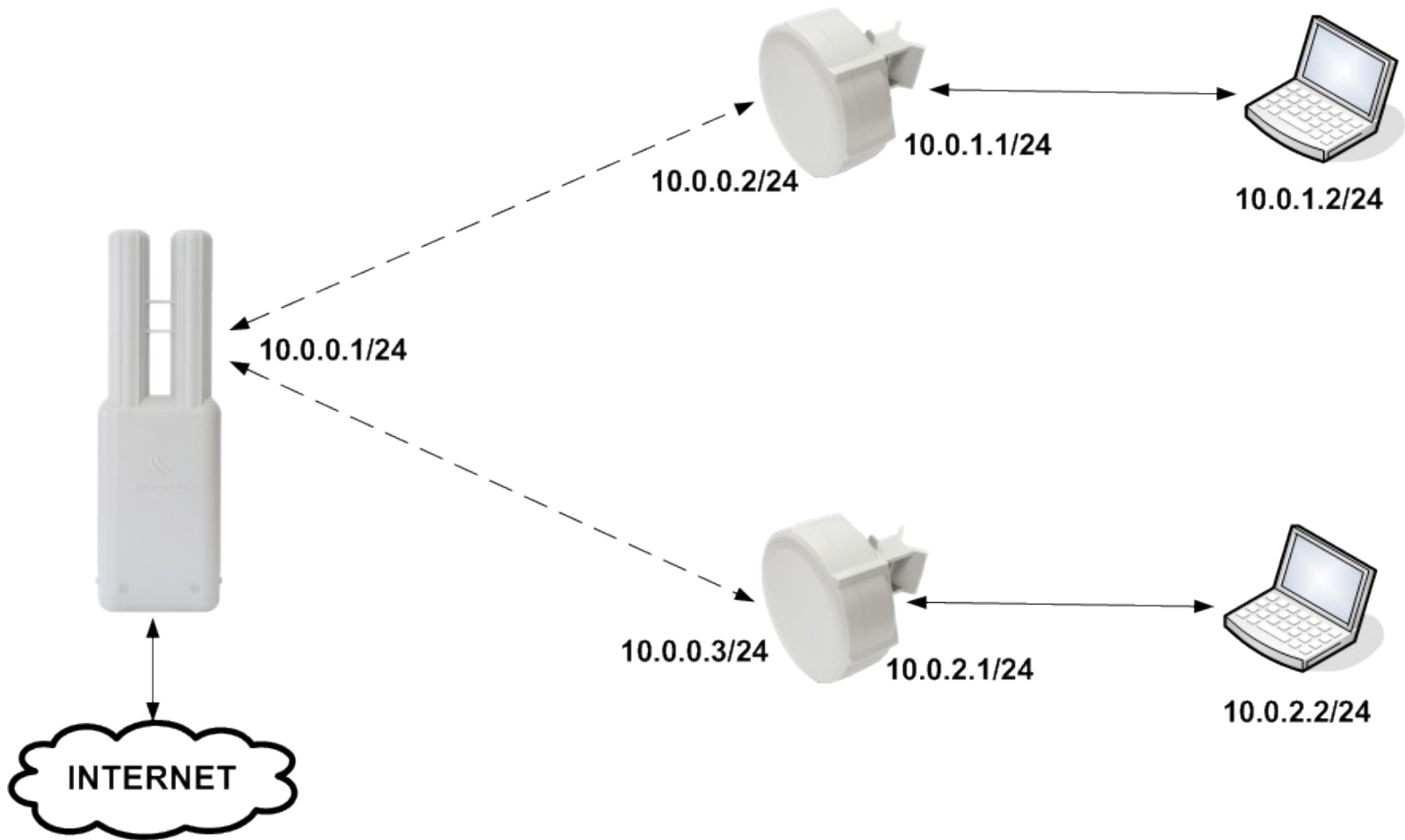
Regular PTMP setup



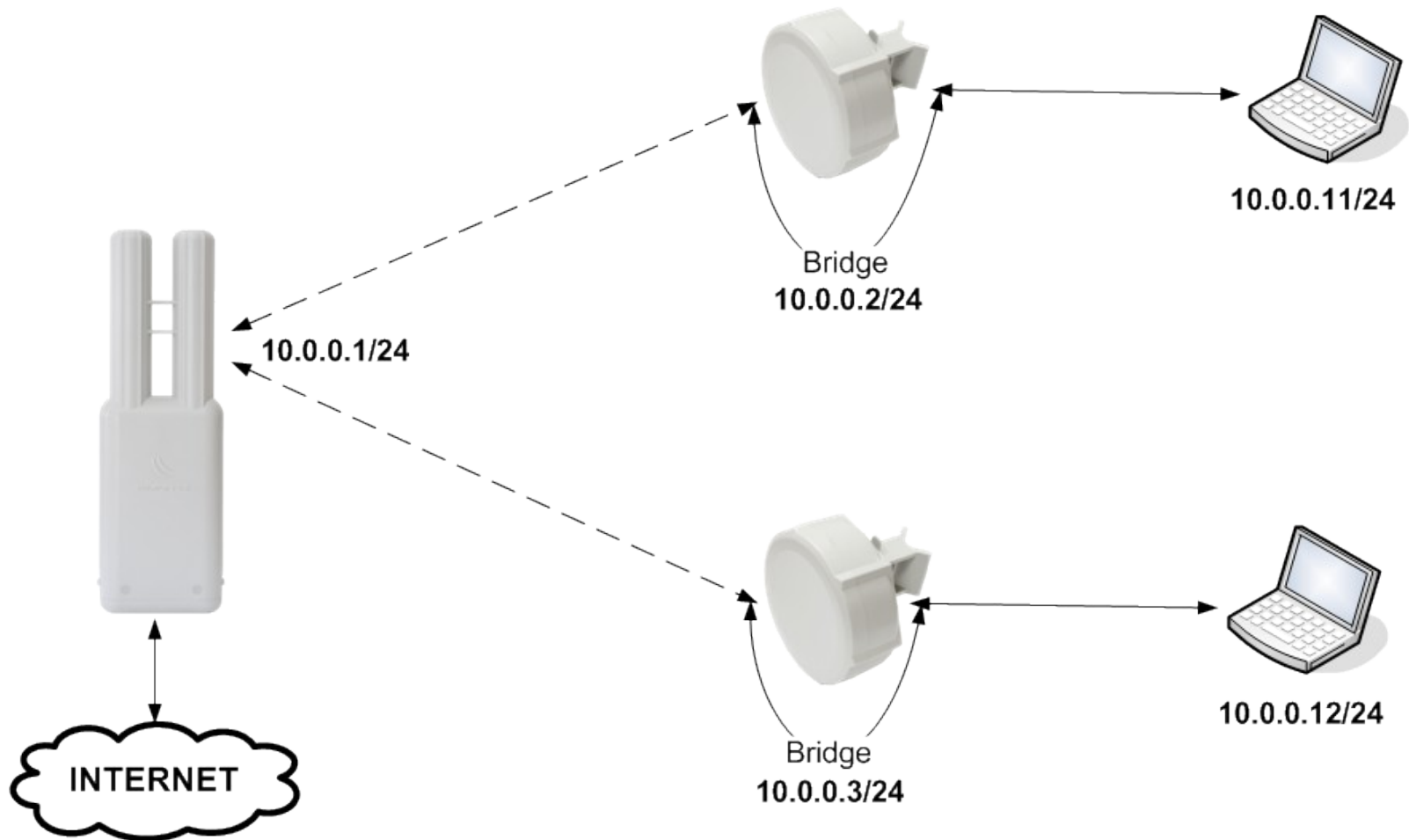
Mesh PTMP setup



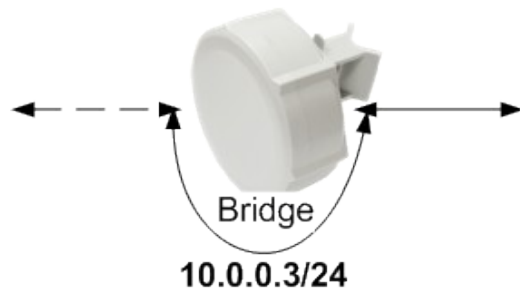
Wireless Setup Type - Routing



Wireless Setup Type - Bridging



Wireless Setup Types



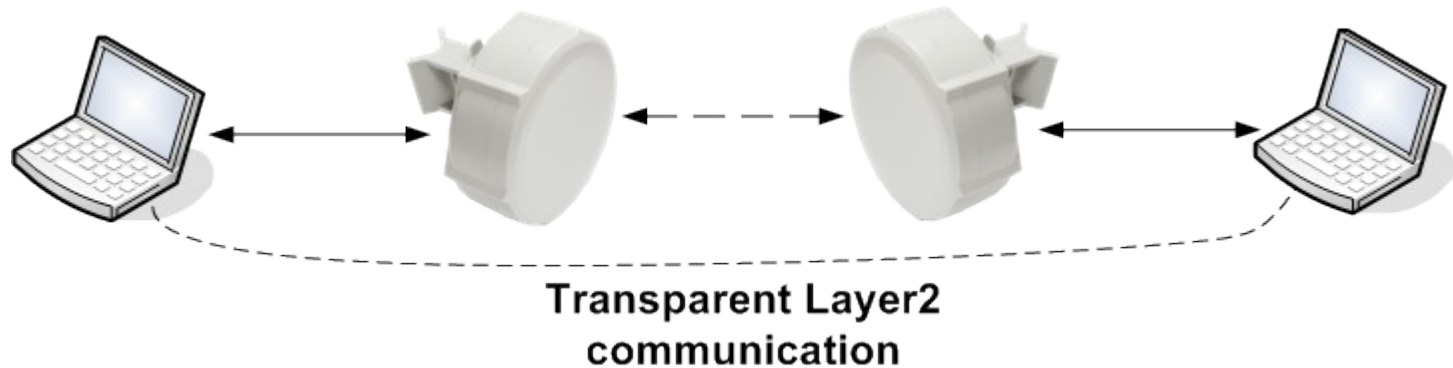
- **Bridging**

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

- **Routing**

- Advantage
 - No broadcast traffic or flood that could lower wireless network performance
- Disadvantage
 - More configuration needed: multiple IP networks or use of routing protocols

Transparent Wireless Links



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

Transparent Wireless Links Setups

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

Station-pseudobridge

- This mode is not considered true transparent bridge
- Limitations
 - MAC address translation for IPv4 packets by using IPv4-to-MAC mapping table on station
 - single MAC address translation for the rest of protocols
- Should be avoided when possible
- Use only when non RouterOS AP is used

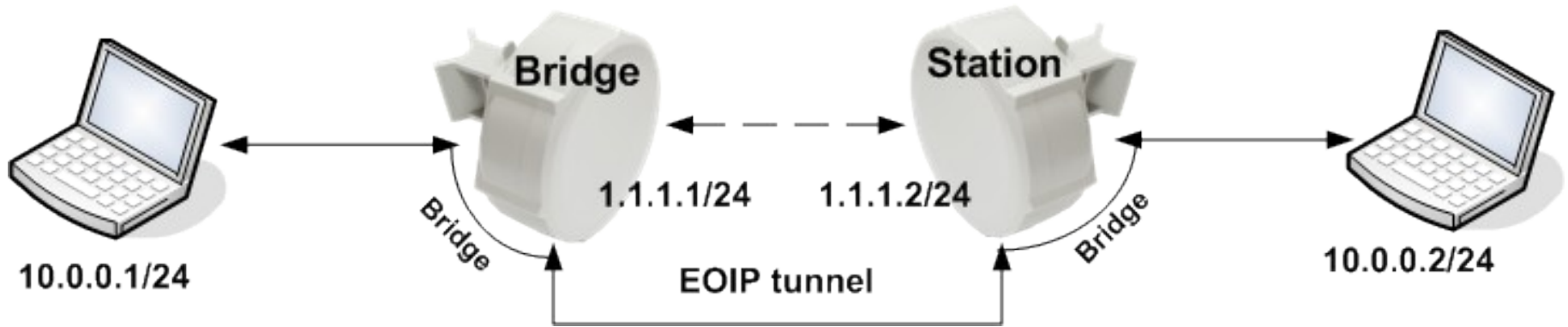
Station-pseudobridge configuration

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

EoIP bridging

- The EoIP protocol encapsulates Ethernet frames in GRE packets (just like PPTP) and sends them to the remote side of the EoIP tunnel
- EoIP adds 42 byte overhead – frame fragmentation will be used

EOIP bridging setup



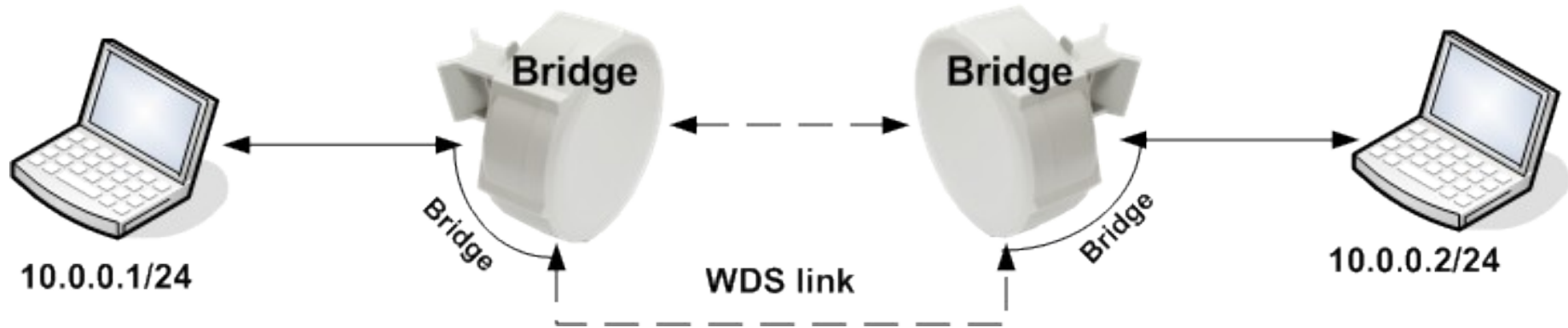
EOIP bridging configuration

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

Bridge <-> Bridge

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

Bridge <-> Bridge setup



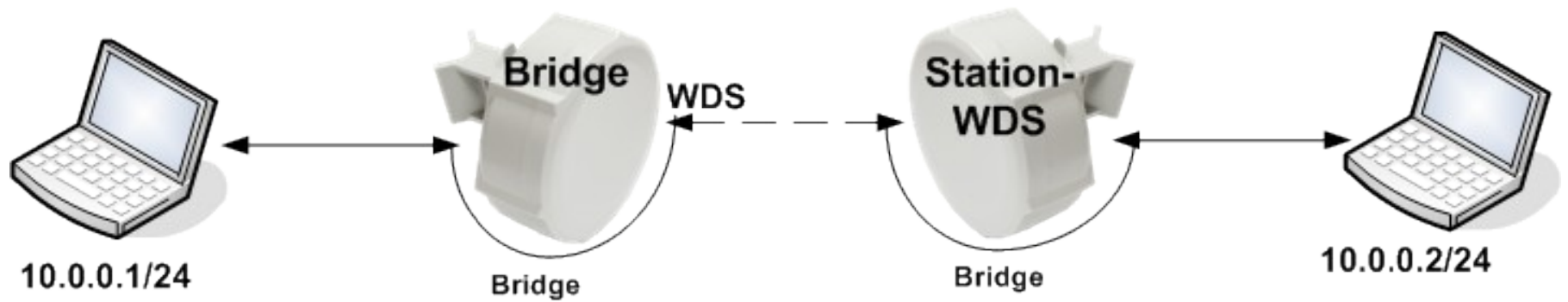
Bridge <-> Bridge configuration

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

Station-wds

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

Station-wds setup



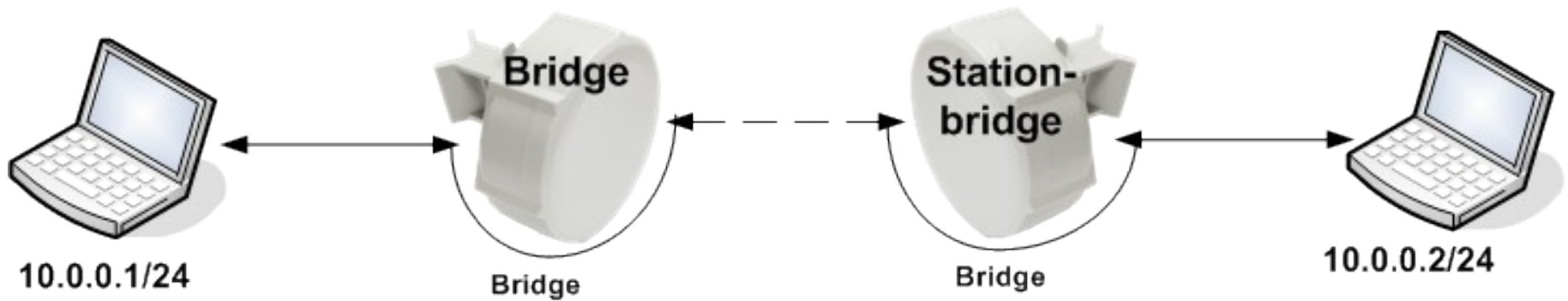
Station-wds configuration

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

Station-bridge

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

Station-bridge setup



Station-bridge configuration

- On AP enable the bridge-mode parameter
- Configure client to use station-bridge mode
- Bridge wireless interface with ethernet interface to make transparent link

Wireless protocol limitations on transparent links

	802.11	ROS	802.11	Nstreme	Nv2
station	V		V	V	V
station-wds			V	V	V
station-pseudobridge	V		V	V	
station-pseudobridge-clone	V		V	V	
station-bridge			V	V	V

Throughput discussion

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

802.11n

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

802.11n 2x20Mhz channel option

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

802.11n Frame Aggregation

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

Upgrade legacy wireless link to 802.11n?

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

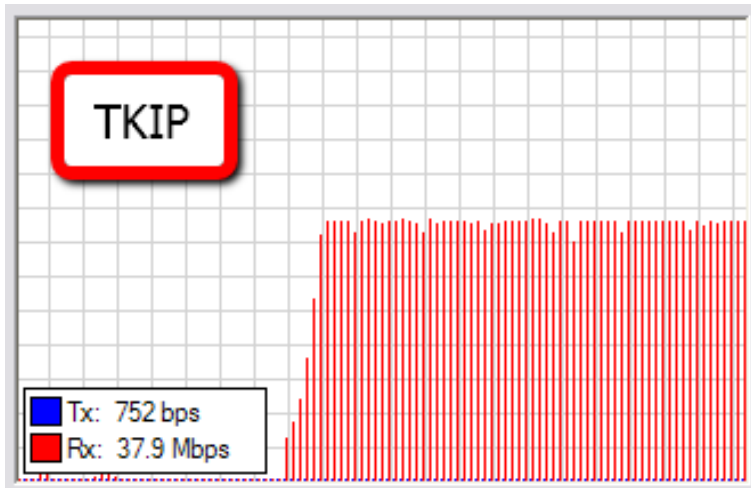
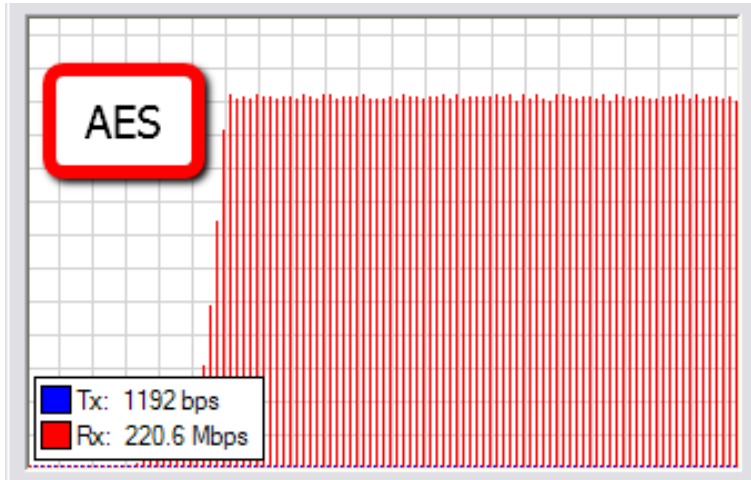
802.11n and WDS

- 802.11n frame aggregation can't be used together with WDS
- Max transmit speed drops from 220Mbps to 160Mbps using WDS (UDP traffic)
- Station-bridge has the same speed limitations as Station-wds
- Avoid using WDS or use Nstreme/Nv2 wireless protocol to overcome this limitation

802.11n Outdoor Setup

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

802.11n speed with encryption



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

AR9300 wireless support

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

AR9300 wireless support

Bandwidth Test (Running)

Test To:

Protocol: udp tcp

Local UDP Tx Size:

Remote UDP Tx Size:

Direction: ▾

TCP Connection Count:

Local Tx Speed: ▾ bps

Remote Tx Speed: ▾ bps

Random Data

User: ▾

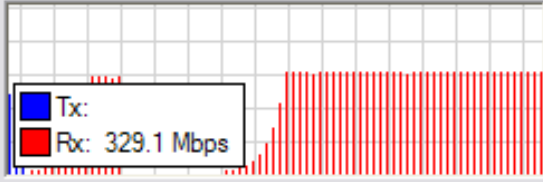
Password: ▾

Lost Packets:

Tx/Rx Current:

Tx/Rx 10s Average:

Tx/Rx Total Average:



running...

Interface <wlan2>

Current Tx Power	Status	Advanced Status	Traffic	...
Band: 5GHz-N				
Frequency: 5450 MHz				
Wireless Protocol: nstreme				
Tx/Rx Rate: 450.0Mbps/450.0Mbps				
SSID: RB800_nv2				
BSSID: 00:0B:6B:7E:50:4D				
Radio Name: 000B6B7E504D				
Tx/Rx Signal Strength: -61/-48 dBm				
Tx/Rx Signal Strength Ch0: -68/-54 dBm				
Tx/Rx Signal Strength Ch1: -64/-50 dBm				
Tx/Rx Signal Strength Ch2: -69/-54 dBm				
Noise Floor: -114 dBm				
Signal To Noise: 66 dB				
Tx/Rx CCQ: 95/100 %				
Overall Tx CCQ: 95 %				
Distance: <input type="text"/>				
RouterOS Version: 5.8				
Last IP: <input type="text" value="2.2.2.1"/>				
<input type="checkbox"/> WDS Link				

NV2

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

TDMA benefits

- More throughput
- Lower latency
- Suited well for Point-to-MultiPoint networks
- Solves hidden node problems

Nv2 compatibility and coexistence with other wireless protocols

- Only RouterOS devices will be able to participate in Nv2 network
- Only RouterOS devices will see Nv2 AP when scanning
- Nv2 network will disturb other networks in the same channel
- Nv2 network may be affected by any (Nv2 or not) other networks in the same channel
- Nv2 enabled device will not connect to any other TDMA based network

Nv2 UDP on RB800

admin@10.5.8.67 (RB800_2) - WinBox v5.8 on RB800 (powerpc)

Uptime: 03:11:35 Memory: 226.6 MiB CPU: 55% Hide Passwords

Safe Mode

Interfaces

Wireless

Bridge

PPP

Switch

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

Radius

Tools

New Terminal

MetaROUTER

Make Supout.rif

Manual

Exit

Registration Connect List Security Profiles

Interface	Uptime	AP	W...	Last Activit...	Tx/Rx Signal ...	Tx/Rx Rate
wlan1	00:05:10	yes	no	0.000	-56/-56	300.0Mbps/300.0Mbps

Resources

Uptime: 03:11:35 OK

Free Memory: 226.6 MiB PCI

Total Memory: 250.3 MiB USB

CPU: e500v2 CPU

CPU Count: 1 IRQ

CPU Frequency: 799 MHz

CPU Load: 55 %

Free HDD Space: 998.5 MB

Total HDD Size: 1044.4 MB

Sector Writes Since Reboot: 266

Total Sector Writes: 2 821 233

Bad Blocks: 0.0 %

Architecture Name: powerpc

Board Name: RB800

Version: 5.8

Interface <wlan1>

Current Tx Power Status Advanced Status Traffic ...

Tx/Rx Rate: 251.1 Mbps / 1216 bps

Tx/Rx Packet Rate: 20 679 p/s / 2 p/s

Tx/Rx Bytes: 20.6 GiB / 2315.3 MiB

Tx/Rx Packets: 14 570 954 / 1 602 653

Tx/Rx Drops: 0 / 0

Tx/Rx Errors: 0 / 0

OK

Cancel

Apply

Disable

Comment

Torch

Scan...

Freq. Usage...

Align...

Sniff...

Snooper...

Reset Configuration

Simple Mode

enabled running slave connected to ess

Nv2 TCP on RB800

admin@10.5.8.67 (RB800_2) - WinBox v5.8 on RB800 (powerpc)

Uptime: 03:33:06 Memory: 226.6 MiB CPU: 51% Hide Passwords

Safe Mode

Interfaces

Wireless

Bridge

PPP

Switch

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

Radius

Tools

New Terminal

MetaROUTER

Make Supout.rif

Manual

Exit

Registration Connect List Security Profiles

Interface	Uptime	AP	W...	Last Activit...	Tx/Rx Signal ...	Tx/Rx Rate
wlan1	00:18:03	yes	no	0.000	-56/-55	300.0Mbps/300.0Mbps

Resources

Uptime: 03:33:06 OK

Free Memory: 226.6 MiB PCI

Total Memory: 250.3 MiB USB

CPU: e500v2 CPU

CPU Count: 1 IRQ

CPU Frequency: 799 MHz

CPU Load: 51 %

Free HDD Space: 998.5 MB

Total HDD Size: 1044.4 MB

Sector Writes Since Reboot: 294

Total Sector Writes: 2 821 261

Bad Blocks: 0.0 %

Architecture Name: powerpc

Board Name: RB800

Version: 5.8

Interface <wlan1>

Current Tx Power Status Advanced Status Traffic ...

Tx/Rx Rate: 120.5 Mbps / 118.1 Mbps

Tx/Rx Packet Rate: 12 188 p/s / 12 015 p/s

Tx/Rx Bytes: 27.3 GiB / 5.5 GiB

Tx/Rx Packets: 19 812 603 / 4 765 454

Tx/Rx Drops: 0 / 0

Tx/Rx Errors: 0 / 0

OK

Cancel

Apply

Disable

Comment

Torch

Scan...

Freq. Usage...

Align...

Sniff...

Snooper...

Reset Configuration

Simple Mode

enabled running slave connected to ess

Wireless disconnection causes

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

Interference from other wireless devices

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

Interference from other wireless devices

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

Clients with low signal level

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

Clients with low signal level

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

High packet retransmission rate

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

High packet retransmission rate

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

Hidden node issue

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

Wireless configuration problems

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

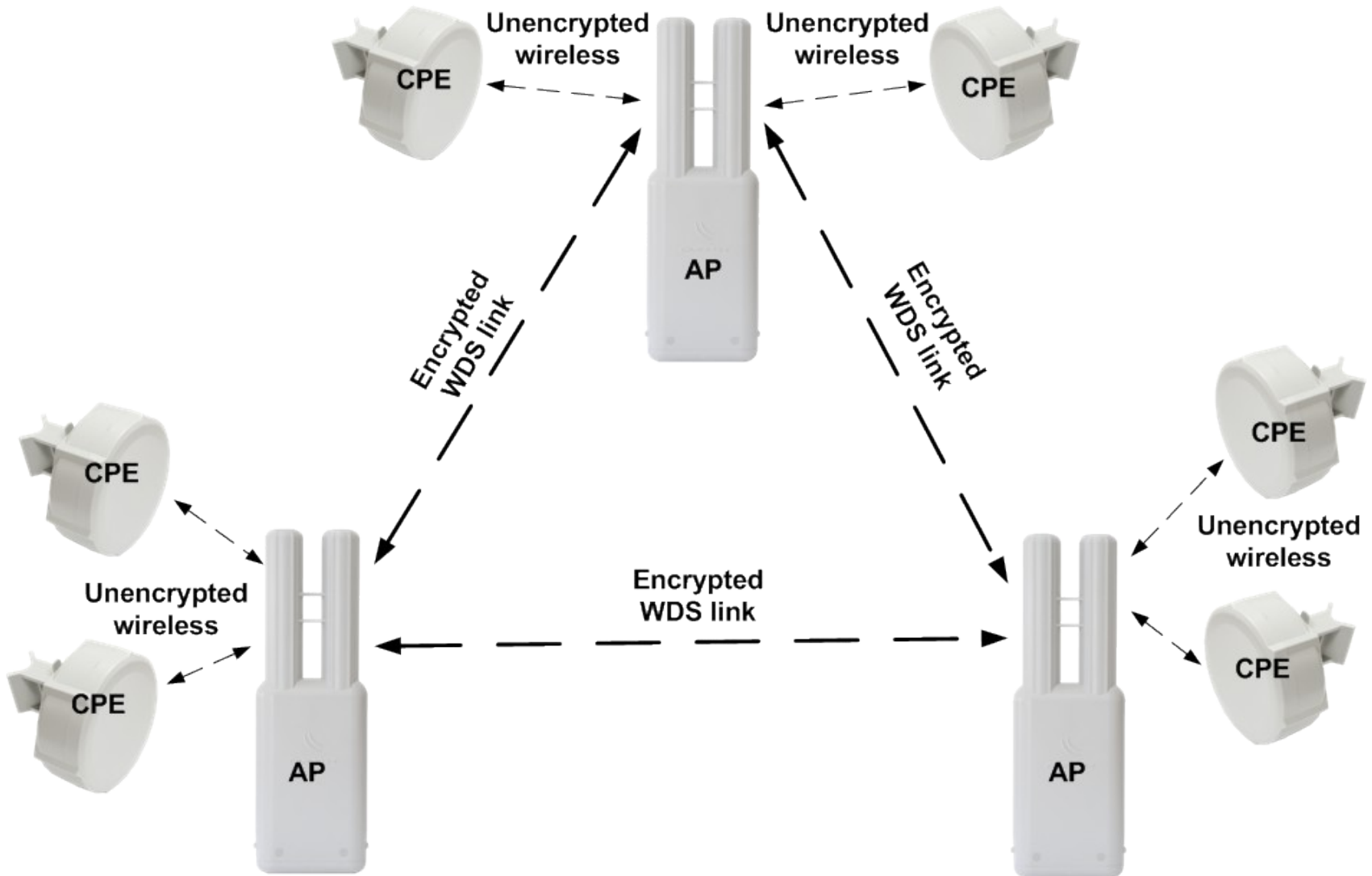
WDS link encryption problem

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

WDS link encryption solution

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

WDS Mesh security and unencrypted clients



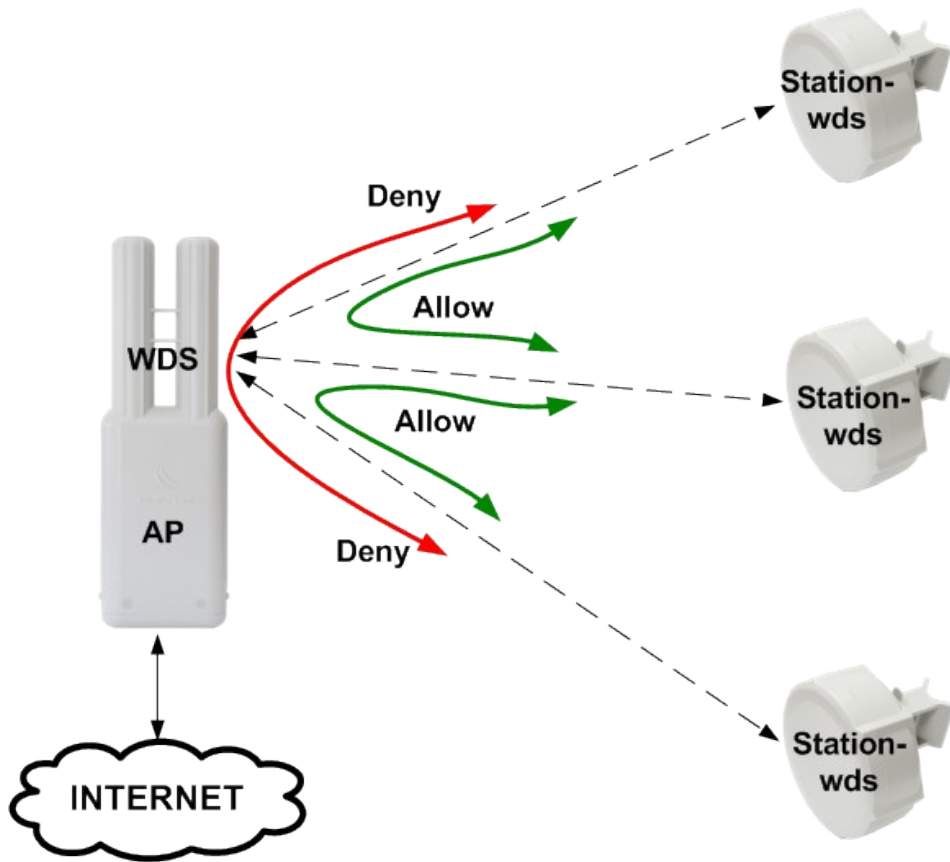
WDS Mesh security and unencrypted clients

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

Dynamic vs. Static WDS

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

Split horizon feature



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

Split horizon feature

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

HT TX/RX chain configuration

Interface <wlan1>

Advanced HT HT MCS WDS Nstreme NV2

HT Tx Chains: chain0 chain1

HT Rx Chains: chain0 chain1

Interface <wlan1>

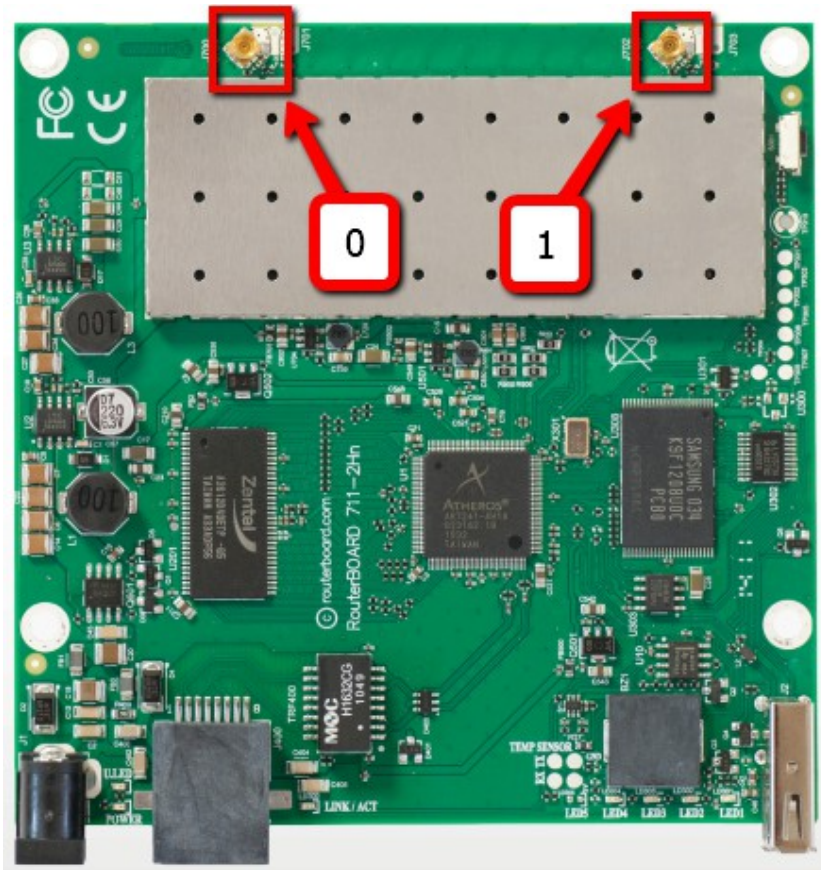
Advanced HT HT MCS WDS Nstreme NV2

HT Tx Chains: chain0 chain1

HT Rx Chains: chain0 chain1

- When board has both antennas connected it is suggested to use all the TX/RX chains to get the best speed and stability
- In order to use only chain1 the chain0 RX should be always enabled in order to make the wireless link to work

RouterBoard wireless boards



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

WPA2 Private Pre Shared Key

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

WPA2 Private Pre Shared Key

The image shows two overlapping configuration windows from a network management interface. The background window is titled "AP Access Rule <00:0C:42:05:36:4C>". It has fields for "MAC Address" (00:0C:42:05:36:4C), "Interface" (wlan1), and "Signal Strength Range" (-120..120). There are also fields for "AP Tx Limit" and "Client Tx Limit", both with dropdown arrows. Checkboxes for "Authentication" and "Forwarding" are checked. The "Private Key" dropdown is set to "none", and a text field next to it contains "0x". A red circle highlights the "Private Pre Shared Key" field, which contains the text "keykeykey2". The foreground window is titled "Security Profile <PSK_security>". It has tabs for "General", "RADIUS", "EAP", and "Static Keys". The "Name" field contains "PSK_security" and the "Mode" dropdown is set to "dynamic keys". Under "Authentication Types", "WPA PSK" and "WPA2 PSK" are checked, while "WPA EAP" and "WPA2 EAP" are unchecked. Under "Unicast Ciphers", "aes ccm" is checked and "tkip" is unchecked. Under "Group Ciphers", "aes ccm" is checked and "tkip" is unchecked. The "WPA Pre-Shared Key" field contains "keykeykey1" and the "WPA2 Pre-Shared Key" field also contains "keykeykey1". There are also fields for "Supplicant Identity" and "Group Key Update" (00:05:00). Buttons for "OK", "Cancel", "Apply", "Copy", and "Remove" are on the right side of the foreground window.

AP Access Rule <00:0C:42:05:36:4C>

MAC Address: 00:0C:42:05:36:4C

Interface: wlan1

Signal Strength Range: -120..120

AP Tx Limit: [dropdown]

Client Tx Limit: [dropdown]

Authentication

Forwarding

Private Key: none [dropdown] 0x [text]

Private Pre Shared Key: keykeykey2

Time: [dropdown]

disabled

Security Profile <PSK_security>

General | RADIUS | EAP | Static Keys

Name: PSK_security

Mode: dynamic keys [dropdown]

Authentication Types

WPA PSK WPA2 PSK

WPA EAP WPA2 EAP

Unicast Ciphers

tkip aes ccm

Group Ciphers

tkip aes ccm

WPA Pre-Shared Key: keykeykey1

WPA2 Pre-Shared Key: keykeykey1

Supplicant Identity: [text]

Group Key Update: 00:05:00

OK

Cancel

Apply

Copy

Remove

Management Frame Protection

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

Management Protection Settings

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

Management Protection key

- Configured with security-profile **management-protection-key** setting
- When interface is in AP mode, default management protection key can be overridden by key specified in access-list or by a RADIUS attribute

Rate-selection – legacy

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

Rate-selection – legacy

Legacy

MCS	Streams	Modulation	Data rate (Mbit/s)			
			20 MHz		40 MHz	
			800ns	400ns	800ns	400ns
0	1	BPSK	6.5	7.2	13.5	15
1	1	QPSK	13	14.4	27	30
2	1	QPSK	19.5	21.7	40.5	45
3	1	16-QAM	26	28.9	54	60
4	1	16-QAM	39	43.3	81	90
5	1	64-QAM	52	57.8	108	120
6	1	64-QAM	58.5	65	121.5	135
7	1	64-QAM	65	72.2	135	150

Modulation	Rate
BPSK	1
QPSK	2
QPSK	5.5
QPSK	11

BPSK	6	8	2	BPSK	13	14.4	27	30
BPSK	9	9	2	BPSK	26	28.9	54	60
QPSK	12	10	2	QPSK	39	43.3	81	90
QPSK	18	11	2	16-QAM	52	57.8	108	120
16-QAM	24	12	2	16-QAM	78	86.7	162	180
16-QAM	36	13	2	64-QAM	104	115.6	216	240
64-QAM	48	14	2	64-QAM	117	128.5	243	270
64-QAM	54	15	2	64-QAM	130	144.4	270	300

Rate-selection – advanced

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

Rate-selection – advanced

Advanced

				Data rate (Mbit/s)				
		MCS	Streams	Modulation	20 MHz		40 MHz	
					800ns	400ns	800ns	400ns
		0	1	BPSK	6.5	7.2	13.5	15
		1	1	QPSK	13	14.4	27	30
		2	1	QPSK	19.5	21.7	40.5	45
Modulation	Rate	3	1	16-QAM	26	28.9	54	60
BPSK	1	4	1	16-QAM	39	43.3	81	90
QPSK	2	5	1	64-QAM	52	57.8	108	120
QPSK	5.5	6	1	64-QAM	58.5	65	121.5	135
QPSK	11	7	1	64-QAM	65	72.2	135	150
BPSK	6	8	2	BPSK	13	14.4	27	30
BPSK	9	9	2	QPSK	26	28.9	54	60
QPSK	12	10	2	QPSK	39	43.3	81	90
QPSK	18	11	2	16-QAM	52	57.8	108	120
16-QAM	24	12	2	16-QAM	78	86.7	162	180
16-QAM	36	13	2	64-QAM	104	115.6	216	240
64-QAM	48	14	2	64-QAM	117	130	243	270
64-QAM	54	15	2	64-QAM	130	144.4	270	300

Wireless-protocol setting

Value	AP	Client
unspecified	establish nstreme or 802.11 network based on old nstreme setting	connect to nstreme or 802.11 network based on old nstreme setting
any	same as unspecified	scan for all matching networks, no matter what protocol, connect using protocol of chosen network
802.11	establish 802.11 network	connect to 802.11 networks only
nstreme	establish Nstreme network	connect to Nstreme networks only
nv2	establish Nv2 network	connect to Nv2 networks only
nv2-nstreme-802.11	establish Nv2 network	scan for Nv2 networks, if suitable network found - connect, otherwise scan for Nstreme networks, if suitable network found - connect, otherwise scan for 802.11 network and if suitable network found - connect
nv2-nstreme	establish Nv2 network	scan for Nv2 networks, if suitable network found - connect, otherwise scan for Nstreme networks and if suitable network found - connect

Bridge MAC address

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

Bridge MAC address

Interface <bridge2>

General STP Status Traffic

Name:

Type:

MTU:

L2 MTU:

MAC Address:

ARP: ▼

Admin. MAC Address: ▼

Interface <bridge2>

General STP Status Traffic

Name:

Type:

MTU:

L2 MTU:

MAC Address:

ARP: ▼

Admin. MAC Address: ▲

Signal reading for each chain

Interface <wlan2>

Nstreme NV2 Status Advanced Status Traffic ...

Band: 5GHz-N

Frequency: 5700 MHz

Tx/Rx Rate: 19.5Mbps/19.5Mbps

SSID: RB800_ar9

BSSID: 00:03:7F:40:81:5C

Tx/Rx Signal Strength: -37/-24 dBm

Tx/Rx Signal Strength Ch0: -39/-26 dBm

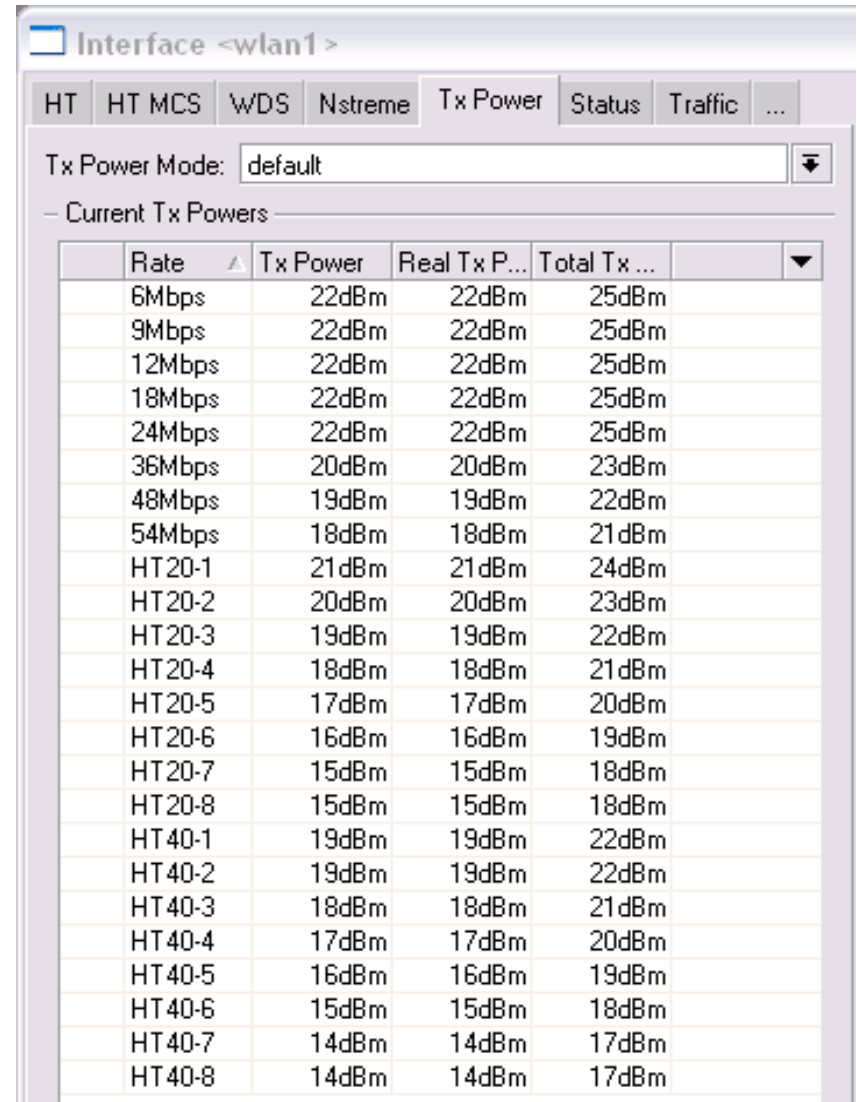
Tx/Rx Signal Strength Ch1: -40/-27 dBm

Tx/Rx Signal Strength Ch2: -51/-41 dBm

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

TX-power for N cards

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



Interface <wlan1 >

HT HT MCS WDS Nstreme Tx Power Status Traffic ...

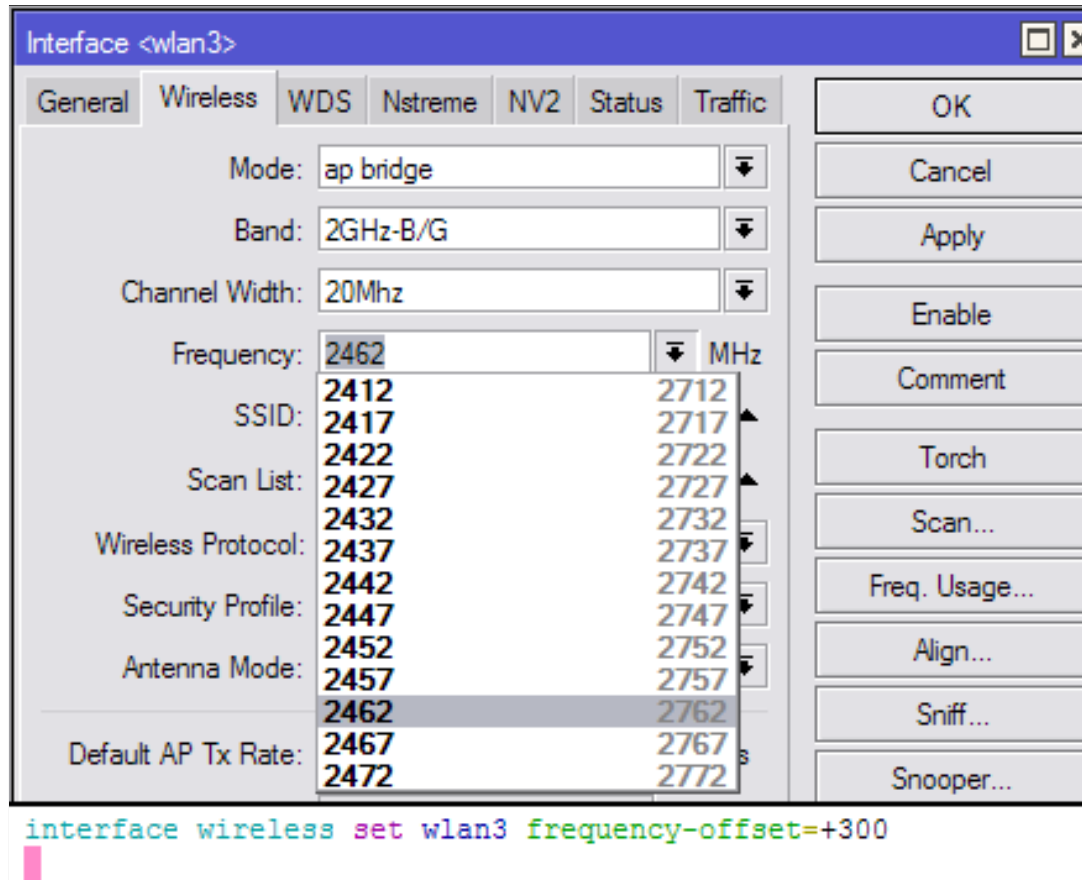
Tx Power Mode: default

– Current Tx Powers

Rate ▲	Tx Power	Real Tx P...	Total Tx ...	▼
6Mbps	22dBm	22dBm	25dBm	
9Mbps	22dBm	22dBm	25dBm	
12Mbps	22dBm	22dBm	25dBm	
18Mbps	22dBm	22dBm	25dBm	
24Mbps	22dBm	22dBm	25dBm	
36Mbps	20dBm	20dBm	23dBm	
48Mbps	19dBm	19dBm	22dBm	
54Mbps	18dBm	18dBm	21dBm	
HT20-1	21dBm	21dBm	24dBm	
HT20-2	20dBm	20dBm	23dBm	
HT20-3	19dBm	19dBm	22dBm	
HT20-4	18dBm	18dBm	21dBm	
HT20-5	17dBm	17dBm	20dBm	
HT20-6	16dBm	16dBm	19dBm	
HT20-7	15dBm	15dBm	18dBm	
HT20-8	15dBm	15dBm	18dBm	
HT40-1	19dBm	19dBm	22dBm	
HT40-2	19dBm	19dBm	22dBm	
HT40-3	18dBm	18dBm	21dBm	
HT40-4	17dBm	17dBm	20dBm	
HT40-5	16dBm	16dBm	19dBm	
HT40-6	15dBm	15dBm	18dBm	
HT40-7	14dBm	14dBm	17dBm	
HT40-8	14dBm	14dBm	17dBm	

Frequency-offset feature

- Frequency-offset feature is designed for easier frequency selection on wireless cards with built-in frequency converter



Antenna-mode selection for RB751U and RB751G

- RB 751U and RB751G has 3 built-in wireless antennas
 - Chain0:
 - one antenna for TX
 - one antenna for RX
 - Chain1:
 - one antenna for TX/RX
 - MMCX connector for external antenna
- Note that enabling the external antenna disables the built-in Chain1 antenna

Antenna-mode selection for RB751U and RB751G

Interface <wlan1>

Advanced HT HT MCS WDS Nstreme NV2 ...

HT Tx Chains: chain0 chain1
HT Rx Chains: chain0 chain1

Antenna Mode: antenna b

HT AMSDU Limit: 8192

HT AMSDU Threshold: 8192

HT Guard Interval: any

HT AMPDU Priorities

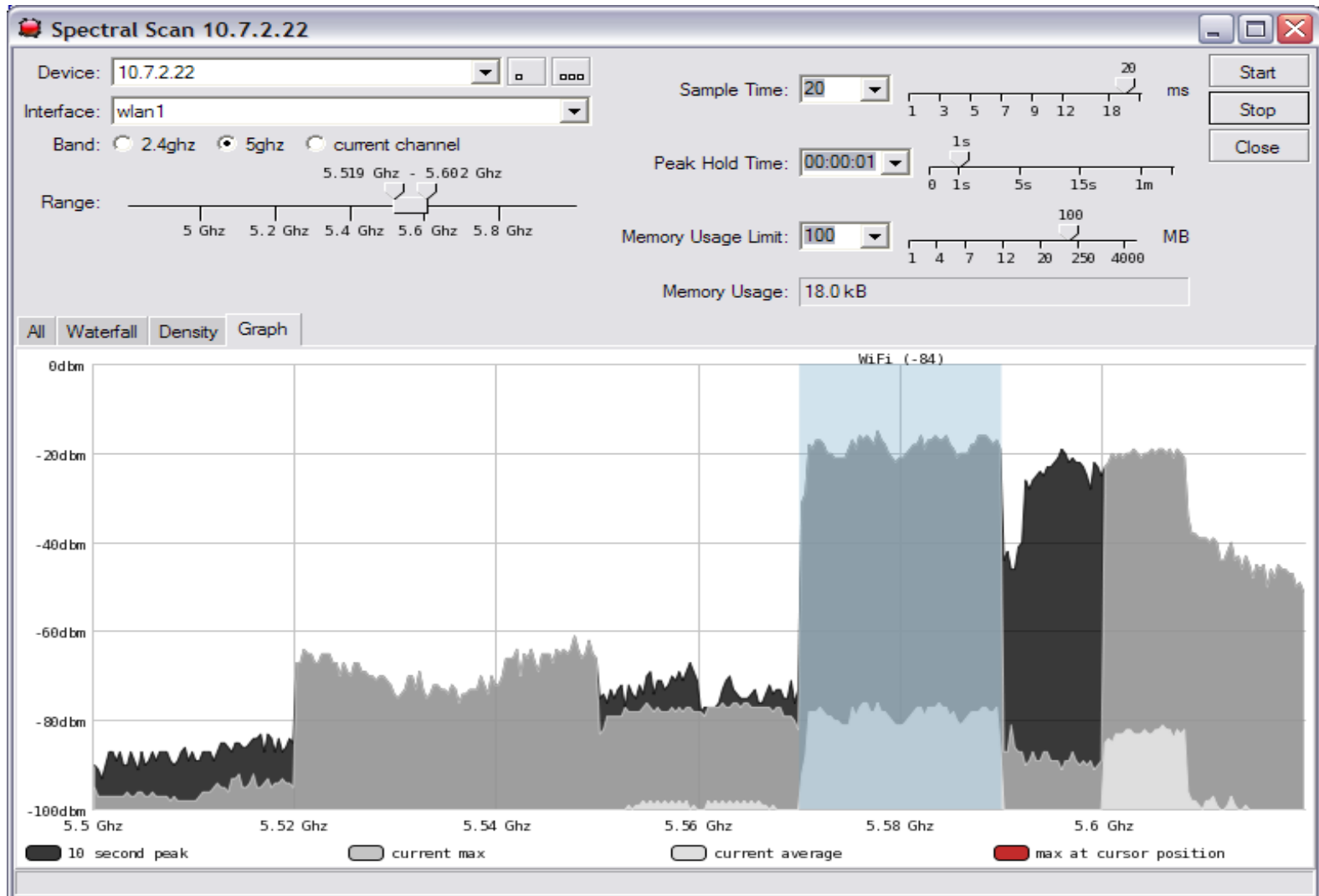
<input checked="" type="checkbox"/> 0	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3
<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/> 7

OK
Cancel
Apply
Disable
Comment
Torch
Scan...
Freq. Usage...
Align...

Spectral Scan/History

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

Spectral Scan using the Dude



Wireless-signal LED feature

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

Wireless-status LED

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

Registration table entries

AP Client <00:0C:42:81:10:E9>

General 802.1x Signal Nstreme NV2 Statistics

Last Activity: 0.000 s

Tx/Rx Signal Strength: -59/-61 dBm

Tx/Rx Signal Strength Ch0: -61/-64 dBm

Tx/Rx Signal Strength Ch1: -65/-64 dBm

Tx/Rx Signal Strength Ch2:

Signal To Noise: 56 dB

Tx/Rx CCQ: 64/73 %

P Throughput: 116330 kbps

- Signal Strengths -

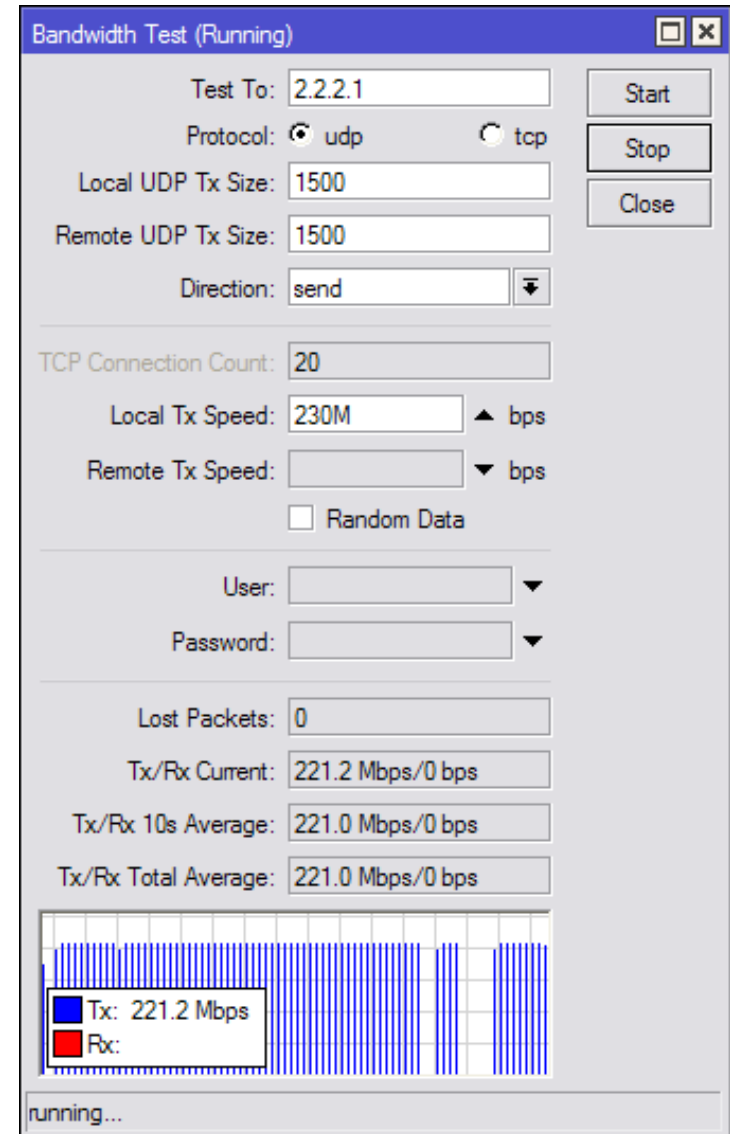
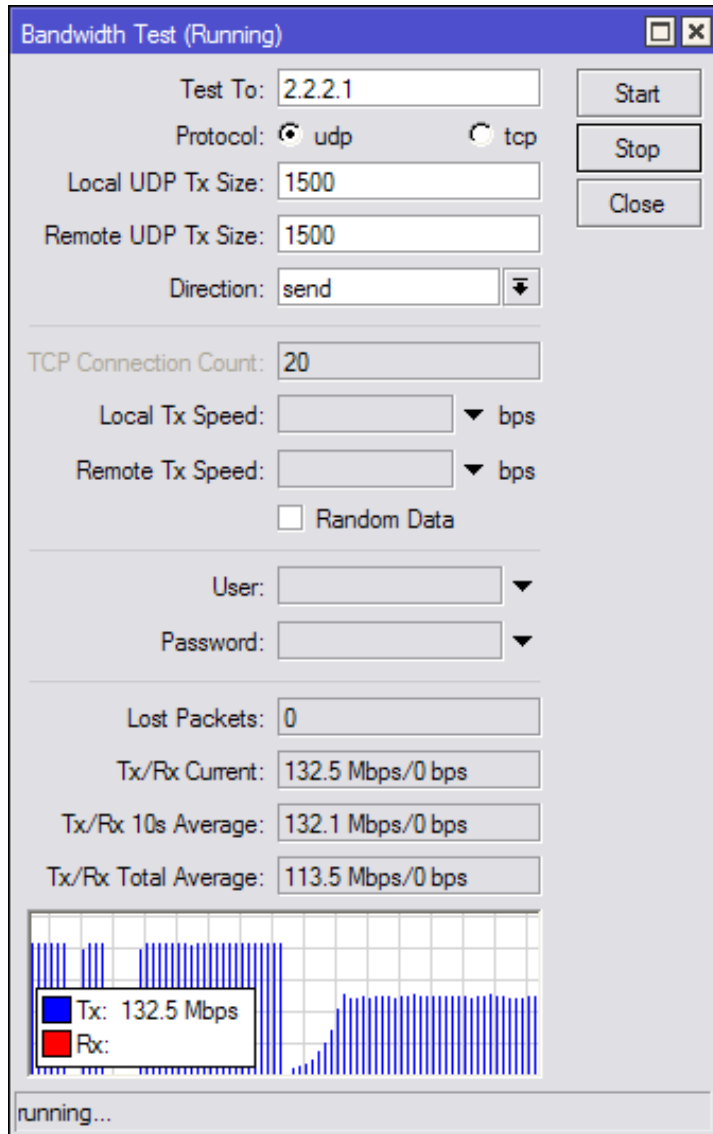
Rate	Strength	Last Measured
48Mbps	-64	00:02:21.32
54Mbps	-62	00:02:23.83
HT20-0	-70	00:02:30.06
HT20-1	-64	00:02:29.21
HT20-2	-59	00:02:28.41
HT20-3	-58	00:02:27.30
HT20-4	-52	00:01:56.56
HT20-5	-59	00:01:56.69
HT20-6	-46	00:01:57.19
HT20-7	-51	00:01:56.78
HT40-0	-63	00:02:29.99
HT40-1	-64	00:02:29.14

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

Wireless Connect-list

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

Bandwidth Test max speed



Wireless Advanced Channels

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

Wireless Advanced Channels

- Custom scan-list options:
 - default, numeric frequency range, advanced channel name, advanced channel list name
- Example: Scan 10 and 20mhz option on the client
 - /interface wireless channels

```
add frequency=5180 width=20 band=5ghz-a list=20mhz-list
add frequency=5200 width=20 band=5ghz-a list=20mhz-list
add frequency=5180 width=10 band=5ghz-a list=10mhz-list
add frequency=5200 width=10 band=5ghz-a list=10mhz-list
```

```
/interface wireless set wlan1 scan-list=20mhz-list,10mhz-list
```

Wireless Advanced Channels

admin@10.5.8.52 (MikroTik) - WinBox v6.0alpha1 on RB800 (powerpc) Uptime: 2d 21:35:58 CPU: 48% Hide Passwords

Safe Mode

Interfaces

- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
- MPLS
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- MetaROUTER
- Make Supout.tif
- Manual
- Exit

Interface <wlan2>

Current Tx Power	Status	Advanced Status	Traffic	...
Band: 5GHz-N				
Frequency: 5360 MHz				
Wireless Protocol: 802.11				
Tx/Rx Rate: 27.0Mbps/405.0Mbps				
SSID: MikroTik1				
BSSID: 00:0C:42:62:B6:45				
Radio Name: 000C4262B645				
Tx/Rx Signal Strength: -56/-55 dBm				
Tx/Rx Signal Strength Ch0: -62/-58 dBm				
Tx/Rx Signal Strength Ch1: -56/-58 dBm				
Tx/Rx Signal Strength Ch2:				
Noise Floor: -111 dBm				
Signal To Noise: 56 dB				
Tx/Rx CCQ: 80/91 %				
Overall Tx CCQ: 80 %				
Distance: 1 km				
RouterOS Version: 6.0alpha1				
Last IP: 8.8.8.1				
<input type="checkbox"/> WDS Link				

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

Bandwidth Test (Running)

Test To: 8.8.8.1 Start
Protocol: udp tcp Stop
Local UDP Tx Size: 1500 Close
Remote UDP Tx Size: 1500
Direction: receive
TCP Connection Count: 20
Local Tx Speed: bps
Remote Tx Speed: bps
 Random Data
User:
Password:
Lost Packets: 2879
Tx/Rx Current: 0 bps/345.1 Mbps
Tx/Rx 10s Average: 0 bps/339.5 Mbps
Tx/Rx Total Average: 0 bps/270.8 Mbps

running...