What to Do With Your Present

Maris Bulans
MikroTik, Latvia

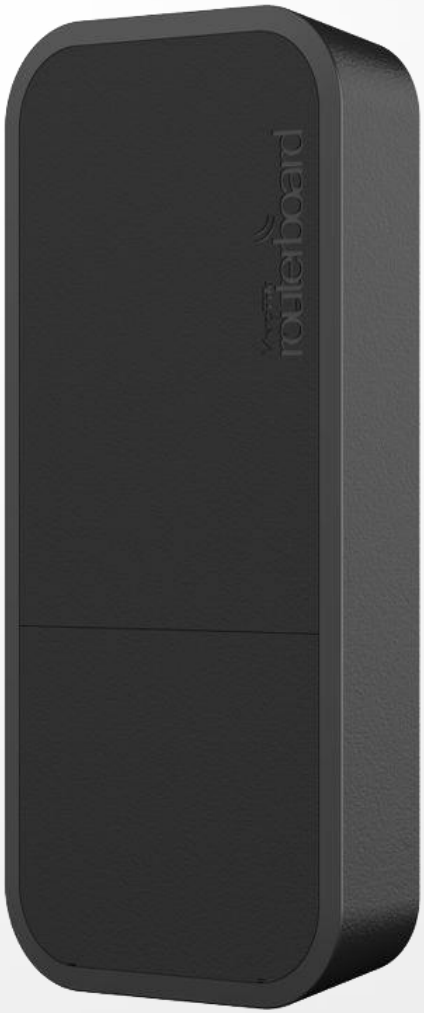
MUM Kazakhstan
June 2016

Overview

- Gift from MikroTik – wAP
- Wireless repeater quick guide
- CAPsMAN overview

wAP

Black and White edition



Features

- CPU 650 MHz
- RAM 64 MB
- Flash 16 MB
- Wireless 802.11b/g/n dual-chain
- Gain 2dBi antennas
- Ethernet 10/100Mbps
- Dimensions 185 x 85 x 30 mm

Features cont

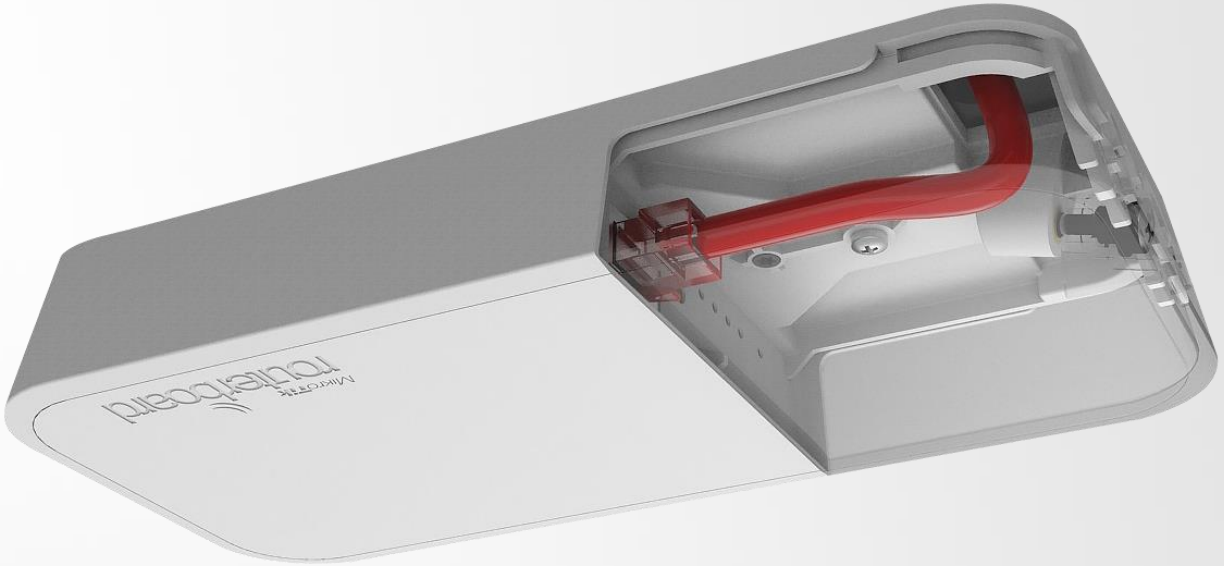
- Wide input Voltage (11-57V)
- 802.3af/at, Passive PoE and power jack
- Low Power Consumption (up to 4W)
- High Operating Temp (-40C to +70C)
- Waterproof case design suitable for indoor and outdoor

Usage Cases

Use it on the wall!

- Wall mounting is easy thanks to the provided drill template and screw anchor. Everything included

Usage Cases



Use it on the ceiling!

- The WAP comes bundled with all the necessary things to be mounted on ceiling
- Cable breakout provides ability to run cable through the ceiling

New wAP ac

- CPU 720 MHz
- RAM 64 MB
- Flash 16 MB
- Wireless 802.11b/g/n dual-chain
- Wireless 802.11a/n/ac triple-chain
- Gain 2dBi antennas
- Ethernet 10/100/1000Mbps
- Voltage 11-57V with 802.3at POE
- Consumption up to 12W
- Operating Temperatures -30C to +70C
- Dimensions 185 x 85 x 30 mm

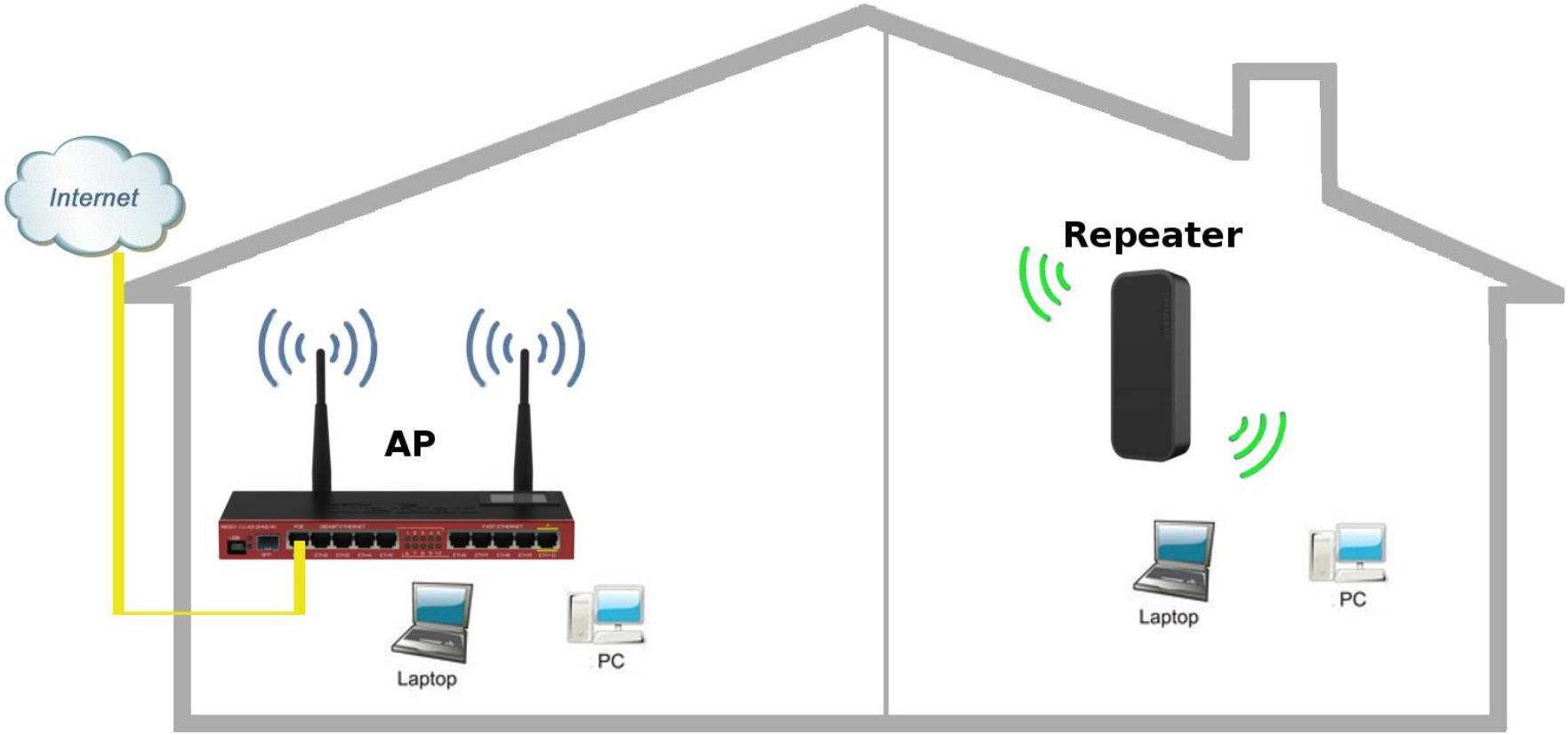
Plug the Cable and Use

- Ether1 configured as WAN port
  - Firewall protection (only ping allowed)
  - Masquerade enabled
  - DHCP client enabled
- Fast-track enabled
- Default local IP: 192.168.88.1/24
- Wireless access point enabled
- SSID: MikroTik-<last 6 chars from MAC>
- DHCP server on wireless AP

Secure the Router

- Connect and set username/password
- Set WPA and WPA2 key to secure AP

Repeater at Home



Repeater at Home

Wireless repeaters extend your wireless network range without requiring you to add any wiring.

Repeater should have two wireless interfaces or new wireless-rep package

How to Connect

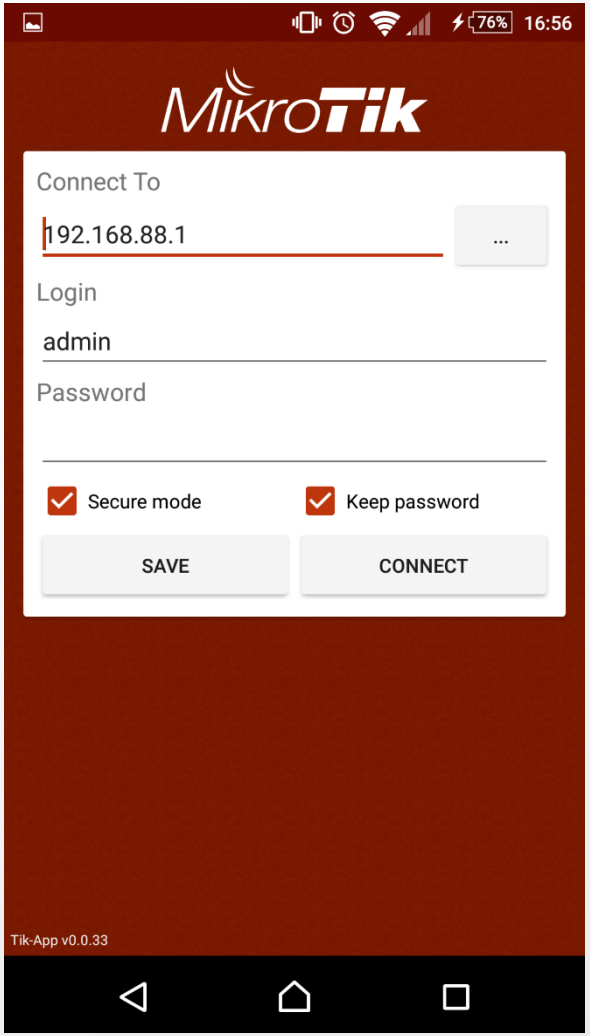
Ethernet (WAN) port is protected

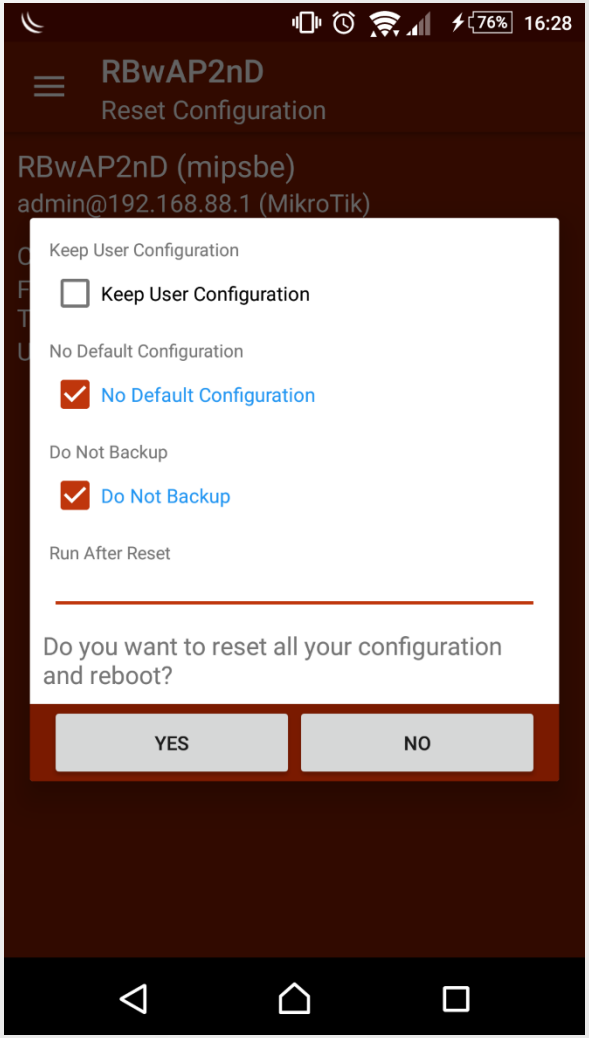
- Connect laptop to wireless and use Winbox/WebfFg, telnet or ssh
- Connect android phone to wireless and use TikApp or WebFig
- Default IP address 192.168.88.1
- Default username: admin w/o password

Default configuration can be switched to CAP mode by holding reset button for 10 seconds.

TikApp

- Sign to testing program, link on Mikrotik forum
- Download TikApp in Play store





Router as station

Configure wireless settings manually to connect to any access point.

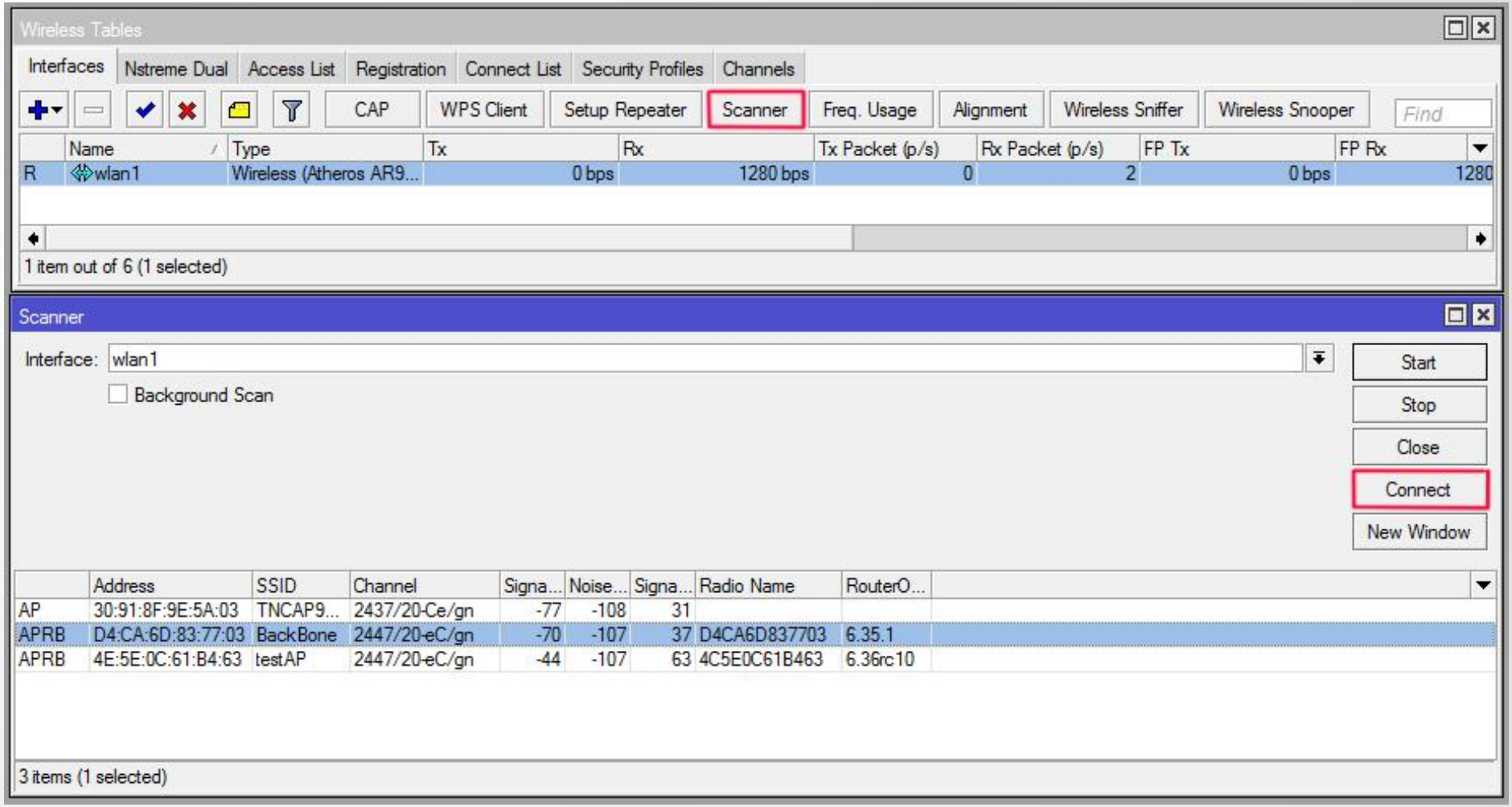
- Configure security profiles (authentication-type, mode, key)
- Configure wireless settings (station mode,frequency, band, SSID)

For repeater setups station mode should be “station-bridge”.

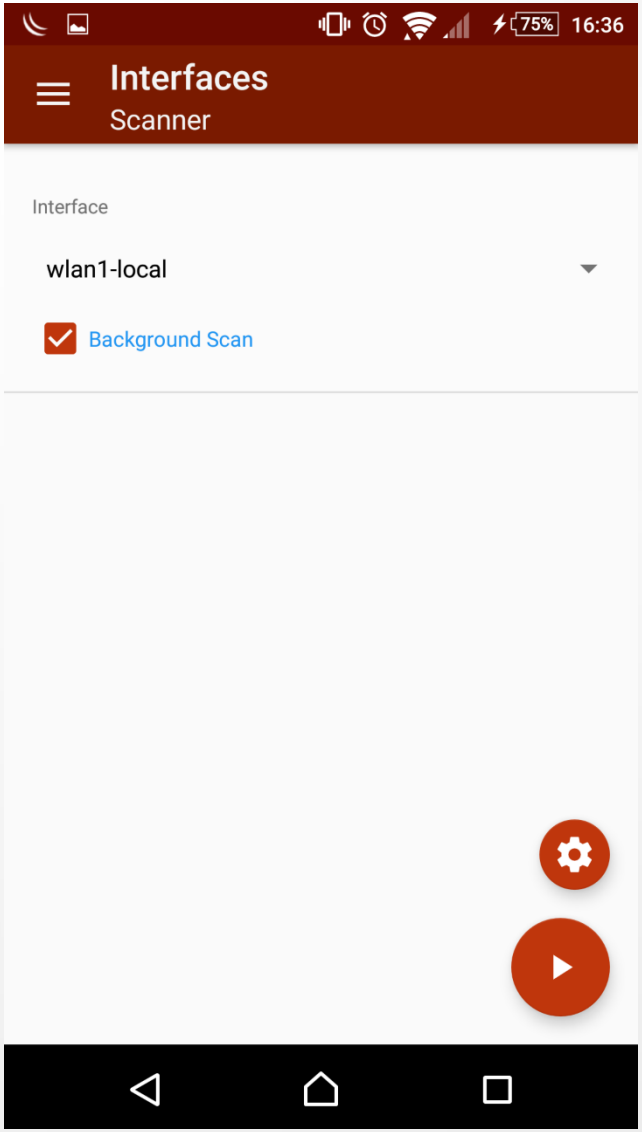
Or use wireless scan feature.

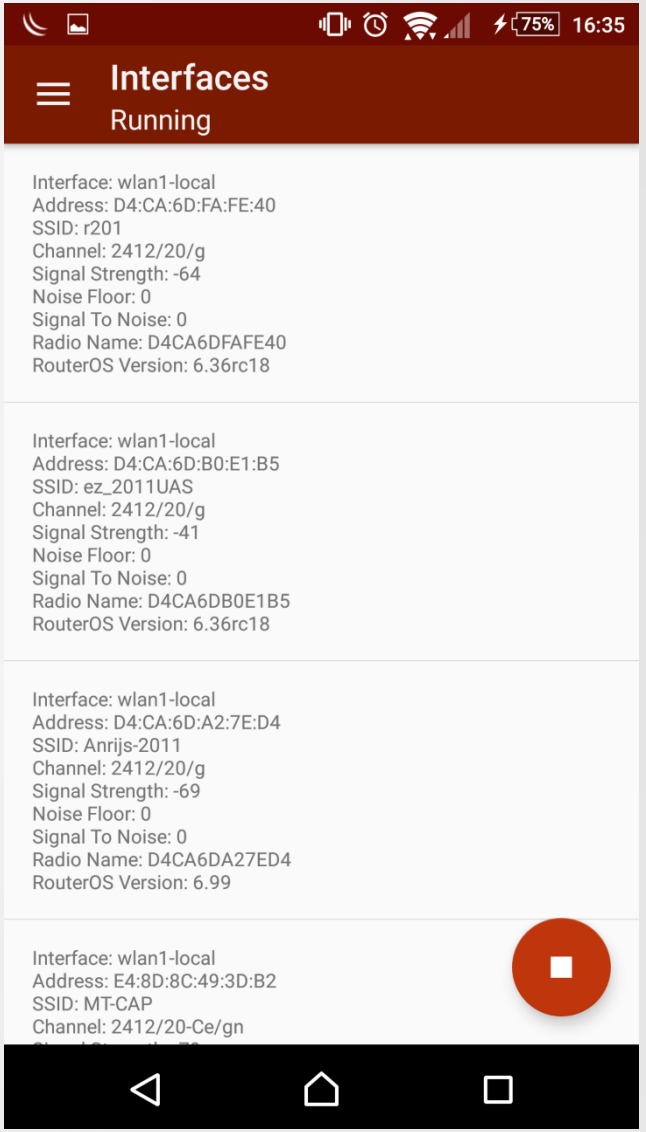
Wireless scan

Fastest way to connect to AP



TikApp scan


75% 16:36
Interfaces
Scanner
Interface
wlan1-local
Background Scan

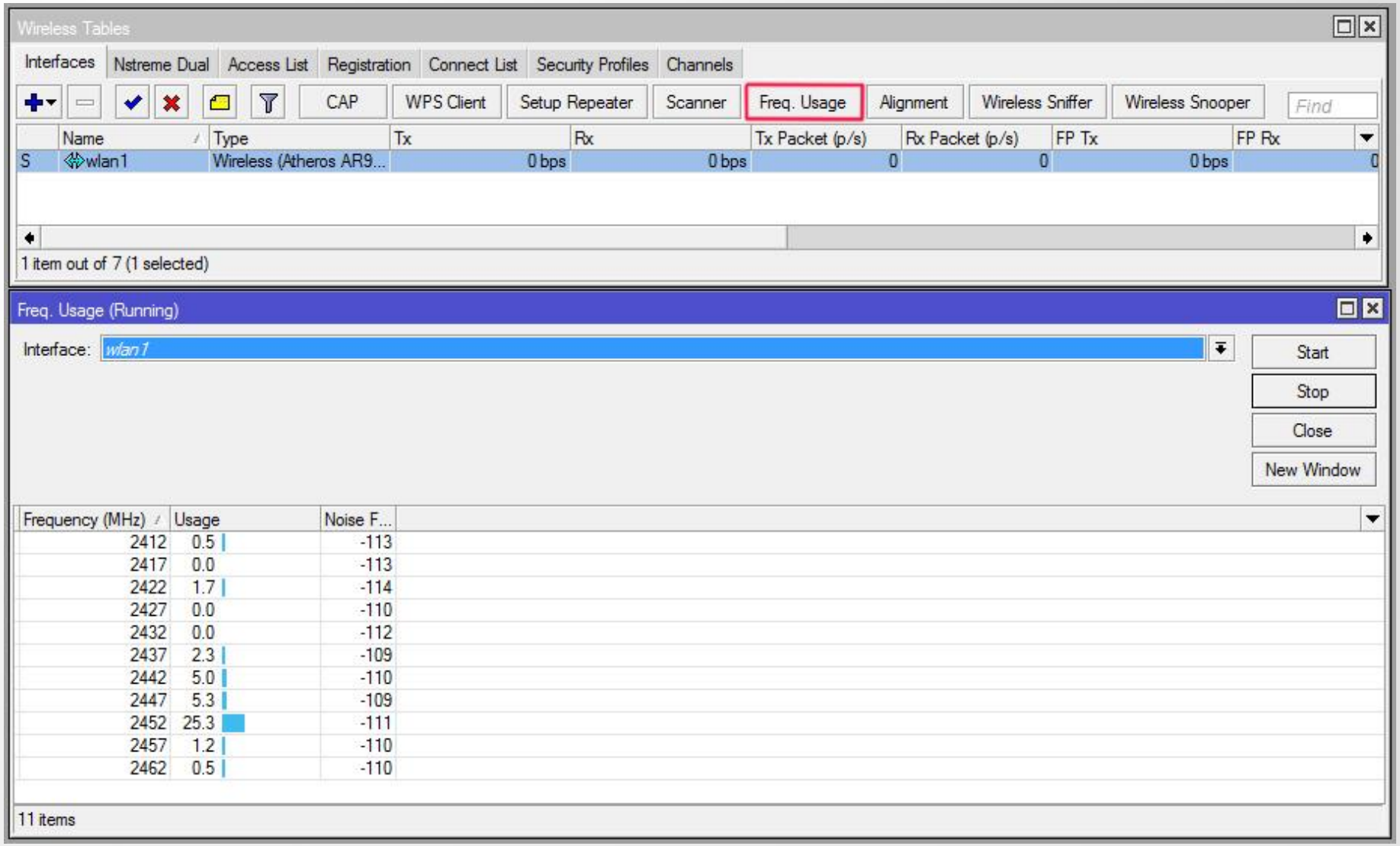

75% 16:35
Interfaces
Running
Interface: wlan1-local
Address: D4:CA:6D:FA:FE:40
SSID: r201
Channel: 2412/20/g
Signal Strength: -64
Noise Floor: 0
Signal To Noise: 0
Radio Name: D4CA6DFAFE40
RouterOS Version: 6.36rc18
Interface: wlan1-local
Address: D4:CA:6D:B0:E1:B5
SSID: ez_2011UAS
Channel: 2412/20/g
Signal Strength: -41
Noise Floor: 0
Signal To Noise: 0
Radio Name: D4CA6DB0E1B5
RouterOS Version: 6.36rc18
Interface: wlan1-local
Address: D4:CA:6D:A2:7E:D4
SSID: Anrijs-2011
Channel: 2412/20/g
Signal Strength: -69
Noise Floor: 0
Signal To Noise: 0
Radio Name: D4CA6DA27ED4
RouterOS Version: 6.99
Interface: wlan1-local
Address: E4:8D:8C:49:3D:B2
SSID: MT-CAP
Channel: 2412/20-Ce/gn

Background Scan

- Supported for 802.11 protocol only
- Working conditions
  - Wireless interface should be enabled
  - For AP mode – when operating on fixed channel
  - For Station mode – when connected to AP
- Supported also on Virtual interfaces
  - Scan is only performed in channel where master interface is running

Frequency scan

Use scan tool, to find the best frequency



Repeater Setup

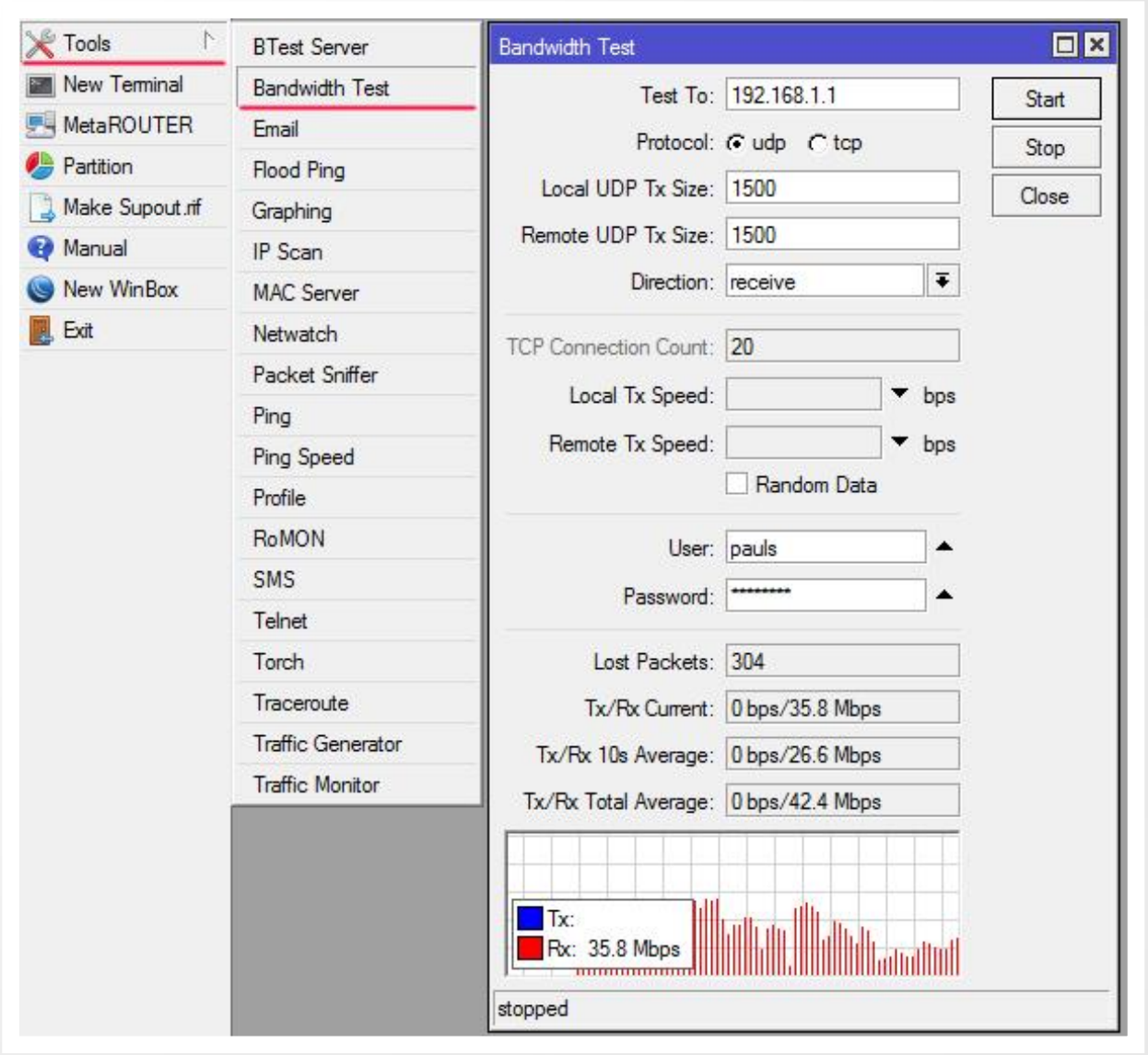
- Download and install **wireless-rep** package
- Add virtual AP interface
- Use the same SSID and security settings
- Add bridge interface with static MAC address
- Bridge physical wireless interface with virtual AP
- Add DHCP client on bridge interface (optionally)

Virtual Wireless Interfaces

- Supported for 802.11 protocol only
- Virtual AP and Client interface can be added on the same physical interface
- Multiple Virtual Wireless interfaces can be added
- Background scan is supported on Virtual Wireless Interfaces and is only performed in channel where master interface is running

Test troughput

Measure troughput between wireless devices



WPS Client Support

- Allows wireless client to get Pre-Shared Key configuration of the AP that has WPS Server enabled
- Gets information from any WPS Server running or can be specified to get only with specific SSID or MAC address
- Received configuration is shown on the screen and can be also saved to a new wireless security profile

Wireless Scan features

- Scan to file
  - Allows to save the scan results in a CSV format file
  - Supported with background scan
- Scan Round setting
  - Allows to do full scan of the scan-list and then stop scanning
  - Useful for remote scans on the clients
  - Supported with background scan as well

Station Roaming support

- Supported for 802.11 protocol only
- While connected to AP station does periodic background scans to look for a better AP
- When a better AP is found station roams to the new AP
- Time intervals between scans becomes shorter when signal becomes worse
- Time intervals between scans becomes longer when signal becomes better

CAPsMAN

- Controlled Access Point system Manager (CAPsMAN)
- Network consists of a number of 'Controlled Access Points' (CAP)
- CAP requires almost no configuration
  - connectivity to CAPsMAN (IP or MAC)
  - wireless lock to capsman:

    ```
    /interface wireless cap set lock-to-caps-man=yes
    ```
- Central processing (default) or local forwarding

CAPsMAN Limitations

- 32 Radios per CAP
- 32 Virtual interfaces per master radio interface
- But unlimited CAPs (access points) supported by CAPsMAN
- CAPsMAN v1 not compatible with v2
- No Nstreme, NV2 support

Thank you!