

# Features and usage examples of wAP device

Maris Bulans  
MikroTik, Latvia

MUM Mongolia  
June 2017

# Features and usage examples of wAP device

Maris Bulans  
MikroTik, Latvia

MUM Mongolia  
June 2017

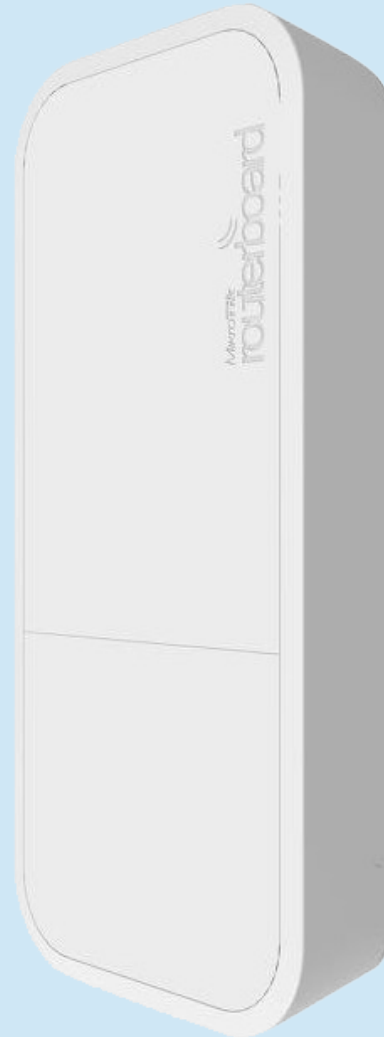
# Overview

- Gift from MikroTik – wAP
- Repeater Setup
- CAPsMAN overview and basic config

# wAP



# Black and White edition



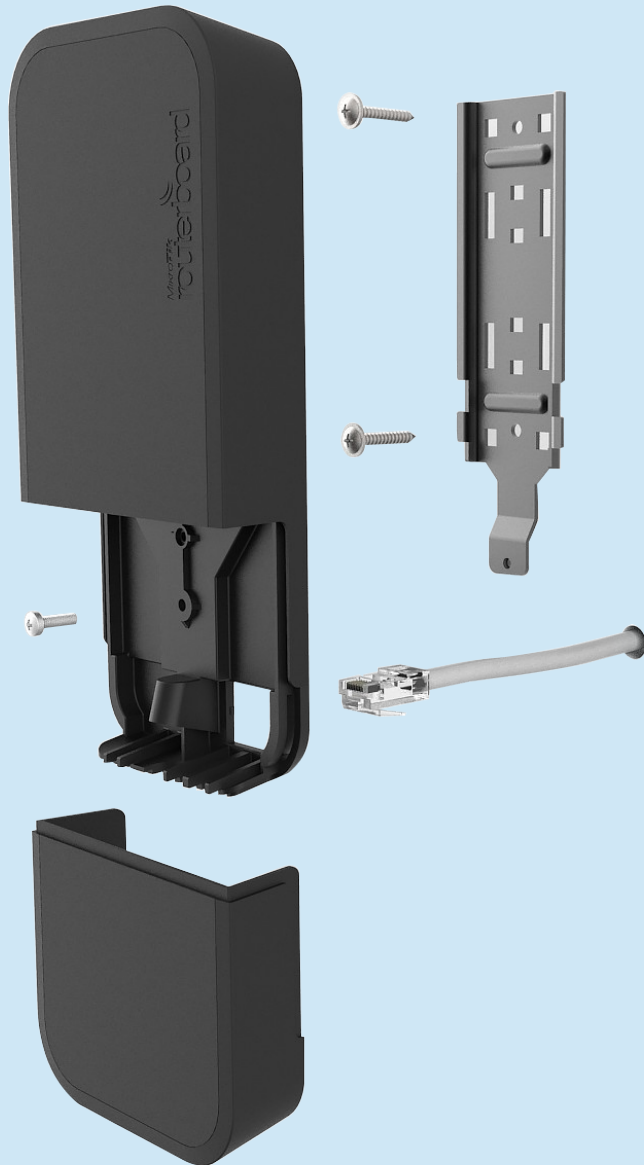
# Features

- 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)
- Weatherproof case design suitable for indoor and outdoor

# Usage Cases

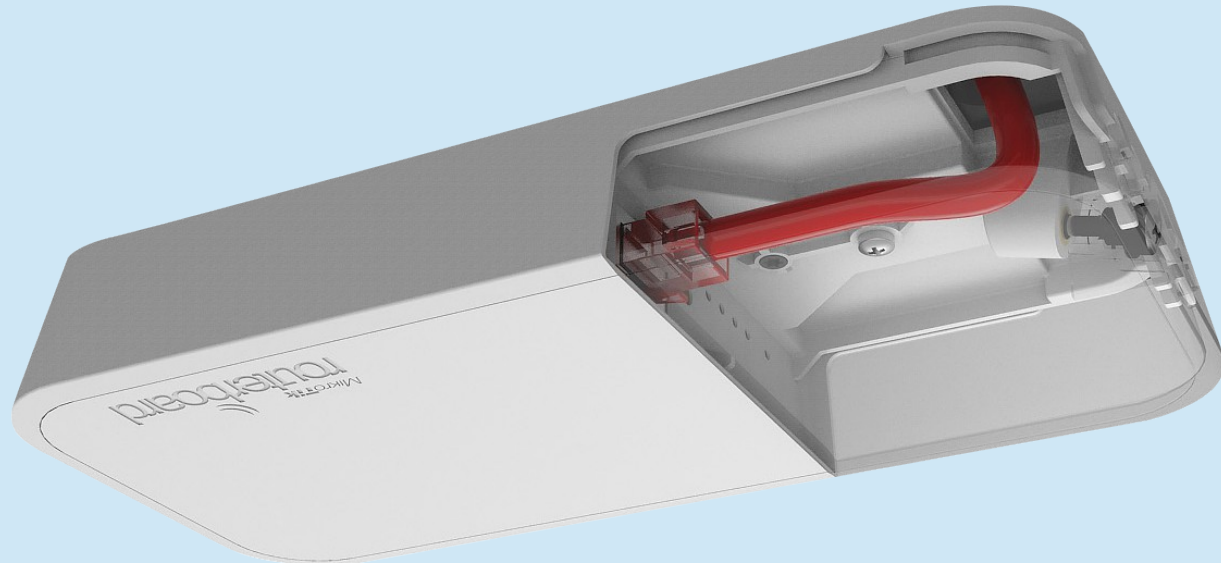


Use it on the wall!

- 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

# Default Configuration

- Ether1 configured as WAN port
  - Firewall protection (only ping allowed)
  - Masquerade enabled
  - DHCP client enabled
  - Neighbour discovery disabled
- 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

# How to Connect

Ethernet (WAN) port is protected

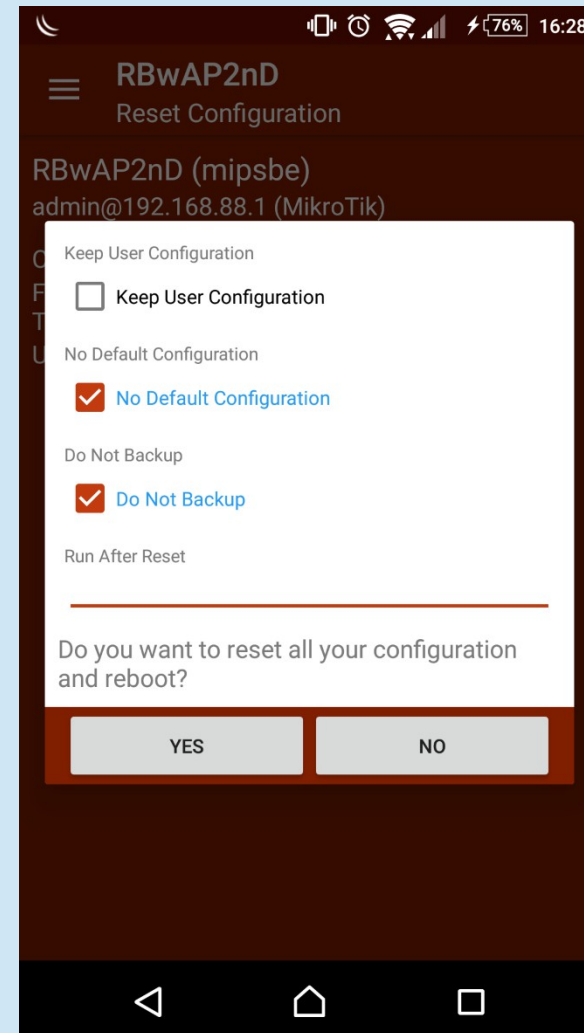
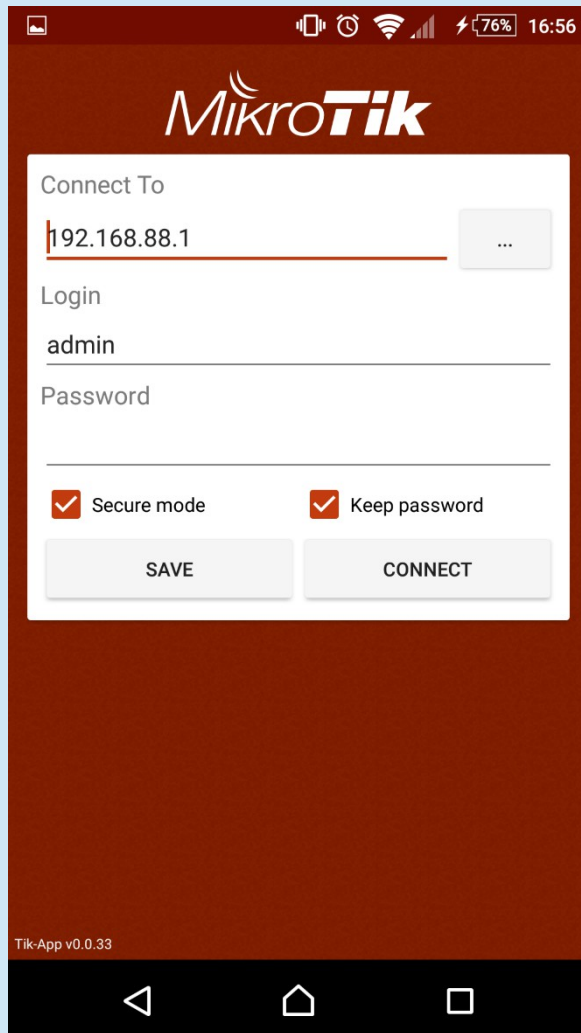
- Connect laptop to wireless and use Winbox/WebFig, telnet or ssh
- Connect android phone to wireless and use TikApp or WebFig
- Default IP address 192.168.88.1
- Default username: admin w/o password

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

- Wireless and ethernet bridged
- DHCP client enabled on bridge interface

# TikApp

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



# Secure the Router

- Connect and set username/password
- Disable 'admin' user
- Set WPA and WPA2 key to secure AP

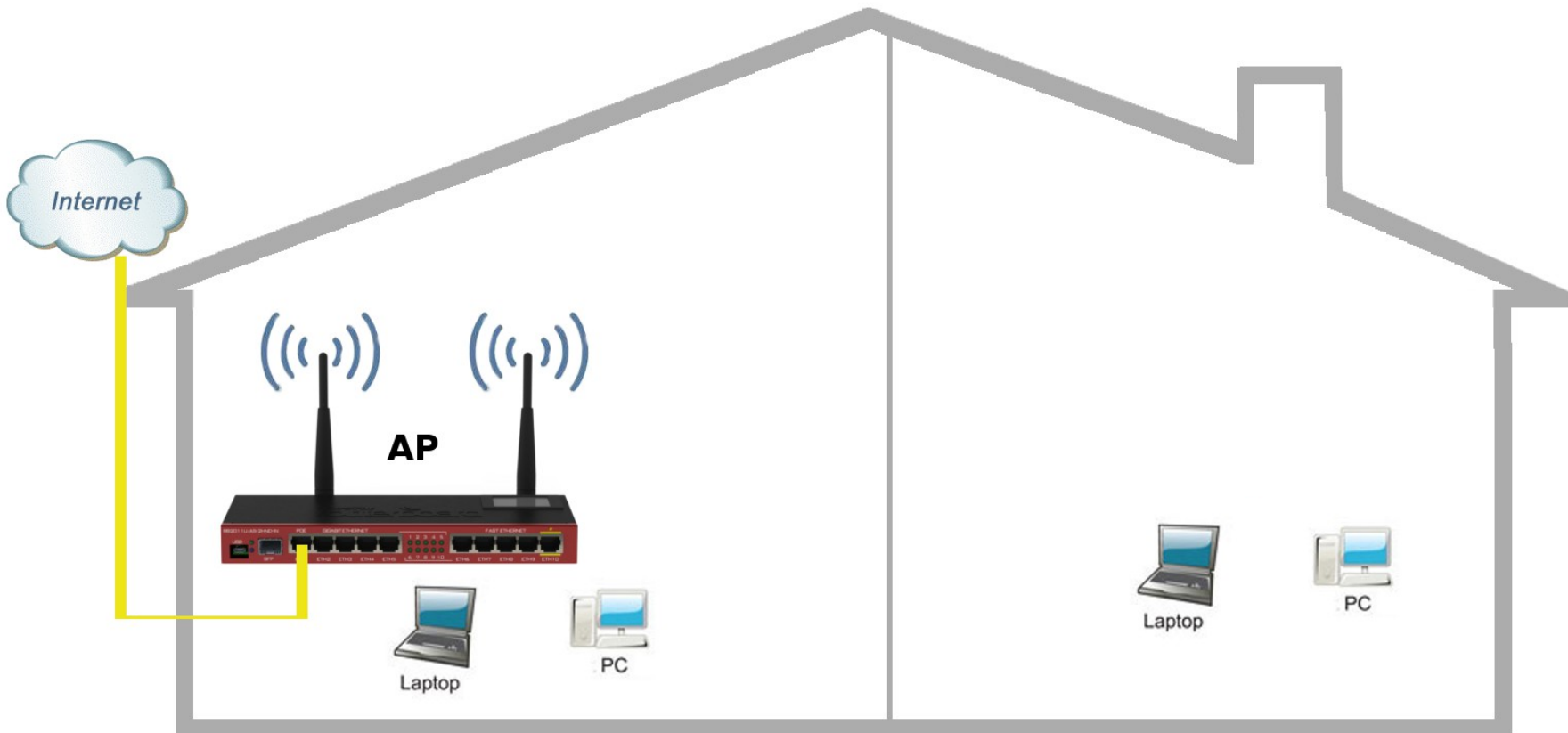
# Repeater at Home

Routers have great coverage, but consumer devices (laptops, mobile phones, refrigerators, toilet seats) does not.

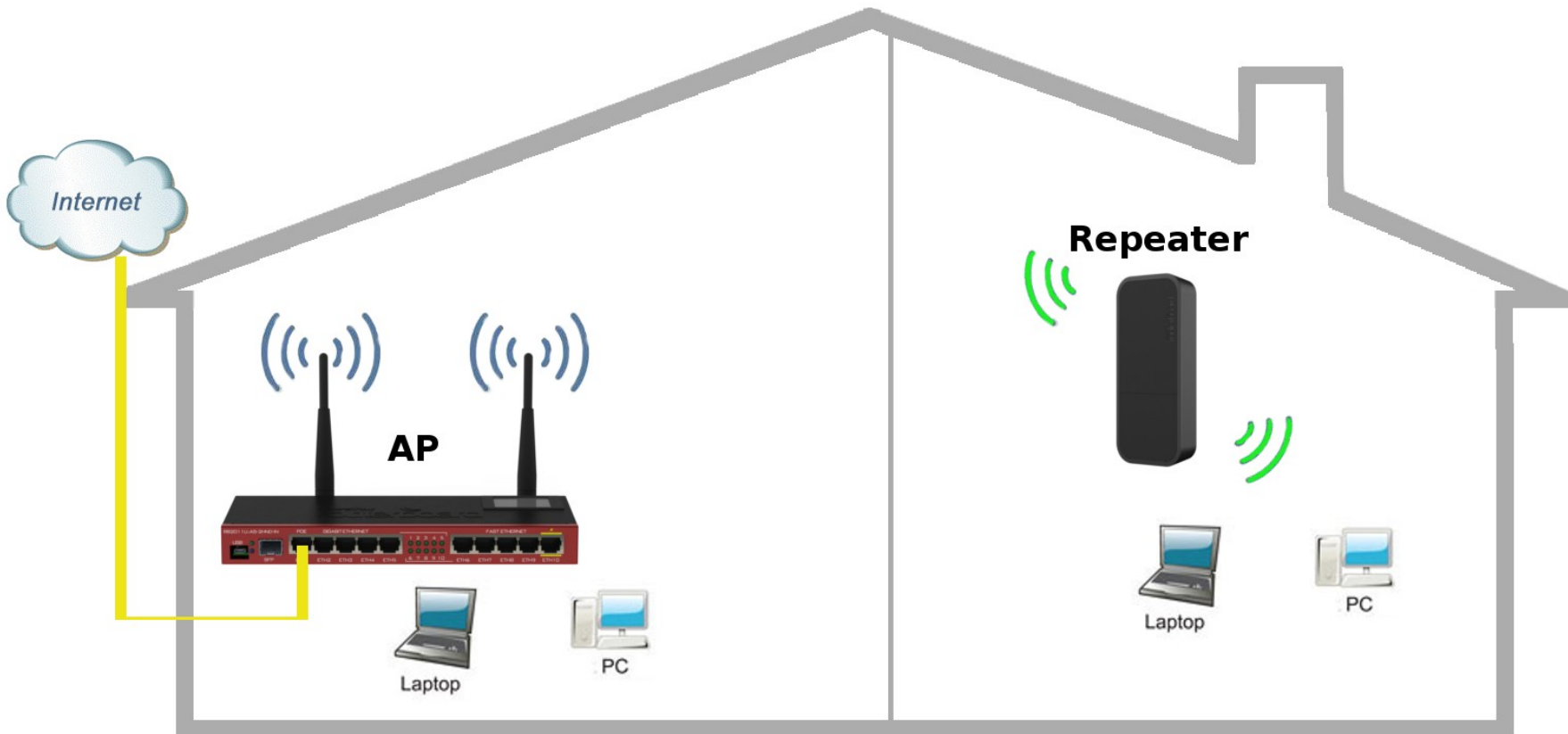
Wireless repeaters extend your wireless network range without requiring you to add any wiring.

Repeater should have two wireless interfaces or set up virtual AP.

# Repeater at Home



# Repeater at Home





# Repeater Setup

Configure wireless settings manually to connect to MikroTik access point:

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

For repeater setups station mode should be “station-bridge” (works only with MT APs).

Or use wireless scan feature.

# Wireless Scan

Fastest way to connect to AP

The image shows two windows from the Mikrotik WinBox interface. The top window is titled "Wireless Tables" and has several tabs: Interfaces, Nstreme Dual, Access List, Registration, Connect List, Security Profiles, and Channels. The "Scanner" tab is highlighted with a red box. Below the tabs are various icons and buttons, including "CAP", "WPS Client", "Setup Repeater", "Scanner" (highlighted), "Freq. Usage", "Alignment", "Wireless Sniffer", and "Wireless Snooper". A table below shows the status of the wlan1 interface.

Name	Type	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx
wlan1	Wireless (Atheros AR9...	0 bps	1280 bps	0	2	0 bps	1280

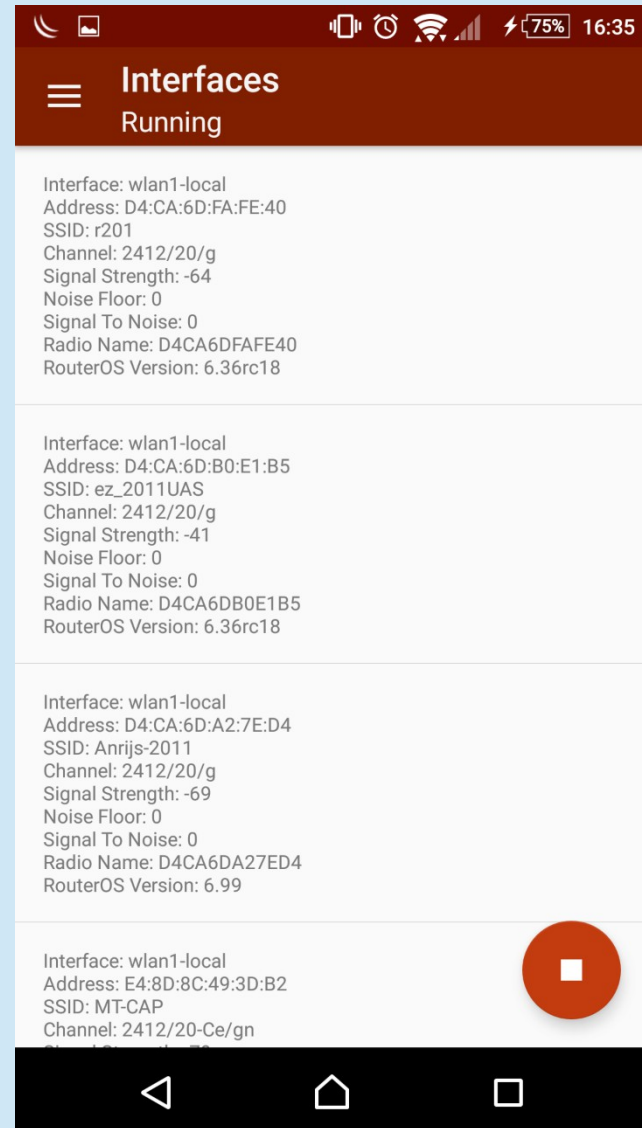
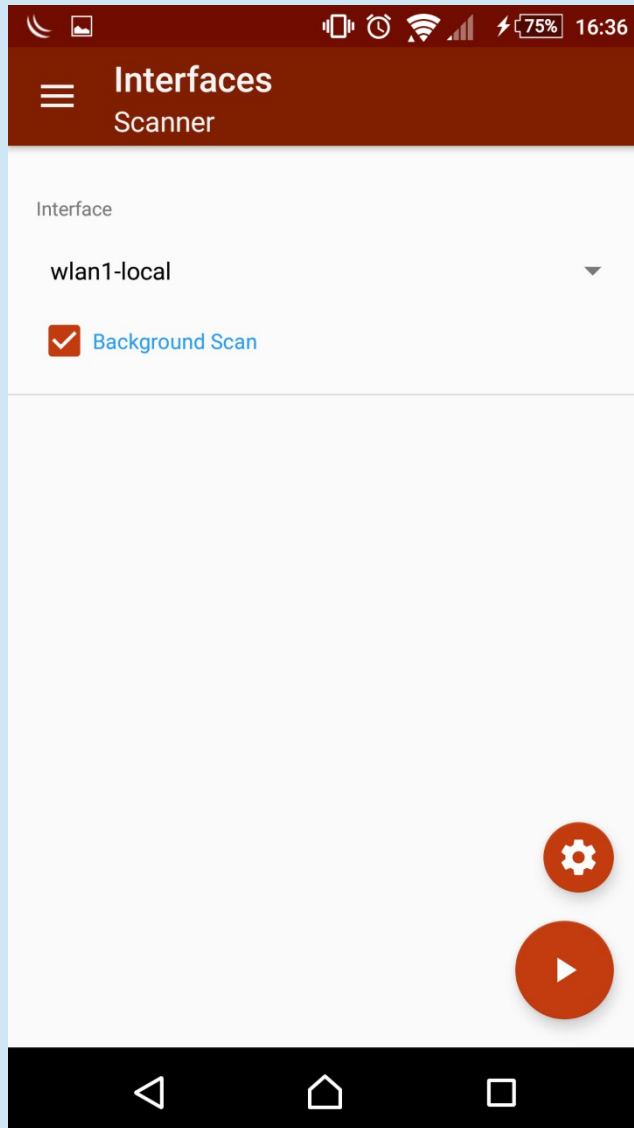
1 item out of 6 (1 selected)

The bottom window is titled "Scanner" and has a dropdown menu for "Interface:" set to "wlan1". There is a checkbox for "Background Scan" which is unchecked. On the right side, there are buttons for "Start", "Stop", "Close", "Connect" (highlighted with a red box), and "New Window". Below these buttons is a table showing scan results.

	Address	SSID	Channel	Signa...	Noise...	Signa...	Radio Name	RouterO...
AP	30:91:8F:9E:5A:03	TNCAP9...	2437/20-Ce/gn	-77	-108	31		
APRB	D4:CA:6D:83:77:03	BackBone	2447/20-eC/gn	-70	-107	37	D4CA6D837703	6.35.1
APRB	4E:5E:0C:61:B4:63	testAP	2447/20-eC/gn	-44	-107	63	4C5E0C61B463	6.36rc10

3 items (1 selected)

# TikApp Scan



# 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
- Allows to save the scan results in a CSV format file

# Repeater Setup

- 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 for management(optional)

# Test throughput

Measure throughput between wireless devices

The screenshot shows a software interface with a 'Tools' menu on the left and a 'Bandwidth Test' window on the right. The 'Tools' menu includes options like 'New Terminal', 'MetaROUTER', 'Partition', 'Make Supout.tif', 'Manual', 'New WinBox', and 'Exit'. The 'Bandwidth Test' window has the following fields and controls:

- Test To: 192.168.1.1
- Protocol:  udp  tcp
- Local UDP Tx Size: 1500
- Remote UDP Tx Size: 1500
- Direction: receive
- TCP Connection Count: 20
- Local Tx Speed: [ ] bps
- Remote Tx Speed: [ ] bps
- Random Data
- User: pauls
- Password: [ ]
- Lost Packets: 304
- Tx/Rx Current: 0 bps/35.8 Mbps
- Tx/Rx 10s Average: 0 bps/26.6 Mbps
- Tx/Rx Total Average: 0 bps/42.4 Mbps

At the bottom of the window, there is a graph showing throughput over time. The legend indicates Tx (blue) and Rx (red). The Rx value is currently 35.8 Mbps. The status at the bottom of the window is 'stopped'.

# WPS Client Support

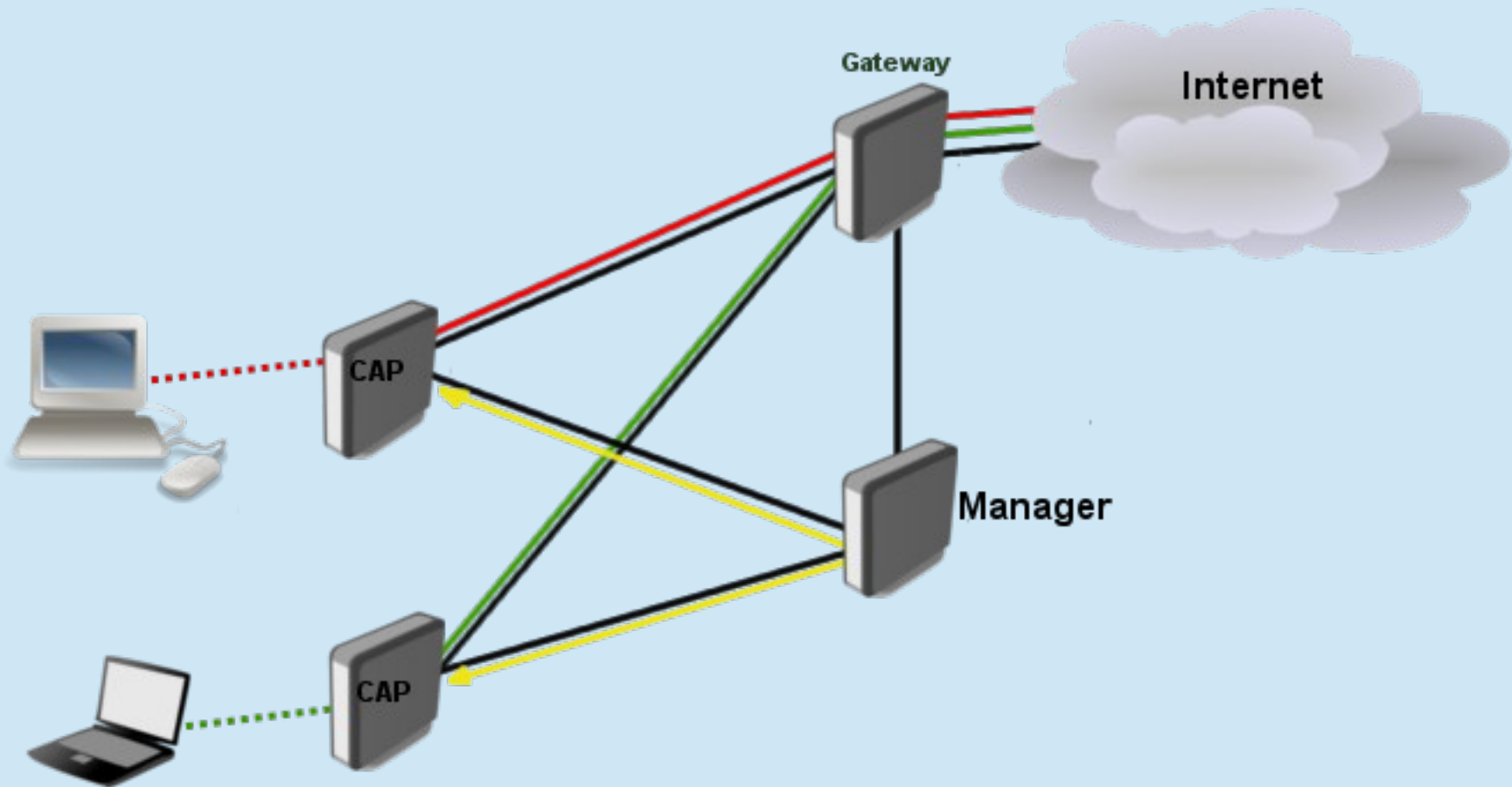
- Allows wireless client to get Pre-Shared Key configuration of the AP that has WPS Server enabled
- Gets information from any WPS Server running or can be specified to get only with specific SSID or MAC address
- Received configuration is shown on the screen and can be also saved to a new wireless security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

# 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
- Packet processing:
  - central (default),
  - local forwarding.



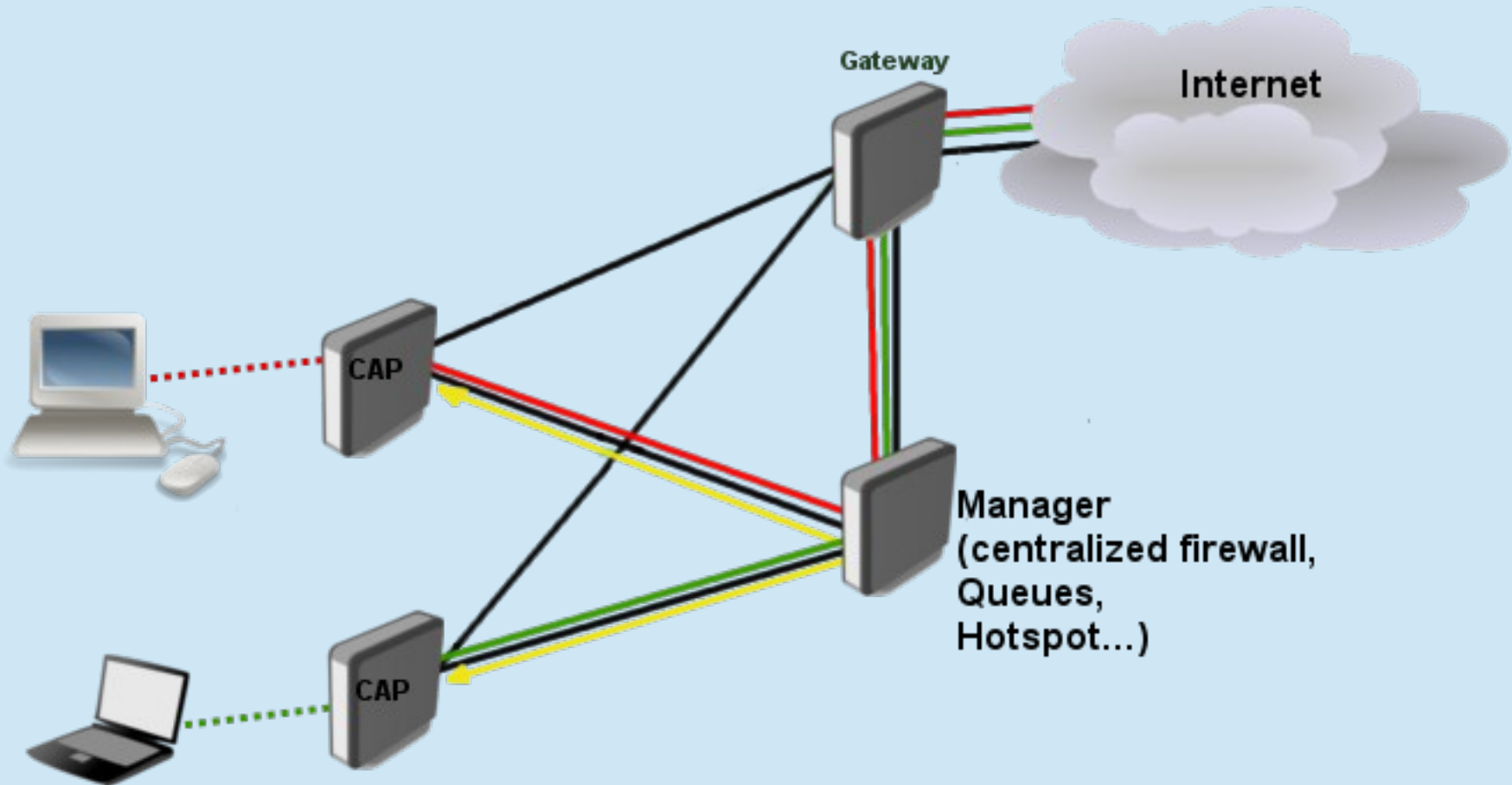
# Local Forwarding



# Local Forwarding

- Pros:
  - Manager can be router with weak CPU
  - Link between manager and gateway not so important
  - Clients do not lose connectivity to internet after CAPsMAN failure
- Cons:
  - Not so friendly for central management
  - Hotspot, firewall, queues, DHCP server in most cases handled locally by CAPs

# Central Forwarding



# Central Forwarding

- Pros:
  - Easy service management on single router
  - Hotspots, DHCP servers, firewall etc can be controlled by groups on single machine
- Cons:
  - Single point of failure (backup CAPsMAN can be set)
  - Hardware must be powerful with fast CPU
  - Link between Manager and Gateway must be stable and fast.

# CAP Configuration

The screenshot displays the Mikrotik WinBox interface for configuring CAP (Certificate Authentication Protocol). The top menu bar includes 'Interfaces', 'Nstreme Dual', 'Access List', 'Registration', 'Connect List', 'Security Profiles', and 'Channels'. The 'CAP' button is highlighted with a red box. A red arrow points from this button to the 'CAP' configuration dialog box.

The 'CAP' configuration dialog box is open, showing the following settings:

- Enabled
- Interfaces: wlan1
- Certificate: CAPsMAN-CA-000C4200635C
- Discovery Interfaces: lo
- Lock To CAPsMAN
- CAPsMAN Addresses: (empty)
- CAPsMAN Names: (empty)
- CAPsMAN Certificate Common Names: (empty)
- Bridge: none
- Static Virtual
- Requested Certificate: CAP-000C4200635C
- Locked CAPsMAN Common Name: (empty)

The background shows a table of wireless interfaces:

Name	Type	Actual MTU	Tx	Rx	Tx Packet (p/s)
--- managed by CAPsMAN					
--- channel: 2427/20-Ce/gn(30dBm), SSID: cap_test_localhost, local forwarding					
RS wlan1	Wireless (Atheros AR...	1500	1200 bps	0 bps	0 bps
wlan2	Virtual		0 bps	0 bps	0 bps

# CAP Configuration

```
/interface wireless cap set enabled=yes interfaces=wlan1
```

Oter parameters depending on  
configuration

```
caps-man-addresses  
discovery-interfaces  
Bridge
```

Default CAP configuration loaded by  
holding reset button for 10 seconds

# CAPsMAN

- CAP and CAPsMAN can be on the same router, set to 'loopback' or 127.0.0.1
- To provision configuration CAPsMAN needs:
  - To get connection from CAP and discover its interfaces
  - To have configuration parameters
  - To have provisioning criteria

CAPsMAN

Provisioning **Configurations** Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Ta

+ - [Folder Icon] [Filter Icon]

Name	SSID	Hide SSID	Load Bal...	Country	Channel	Frequency	Band
cfg1	cap_test_localhost						2ghz-b/g/n

CAPs Configuration <cfg1>

Wireless Channel Rates Datapath Security

Name:

Mode:  ▲▼

SSID:  ▲▼

Hide SSID:

Load Balancing Group:

Distance:  ▼

Hw. Retries:  ▼

Hw. Protection Mode:  ▼

Frame Lifetime:  ▼

Disconnect Timeout:  ▼

Keepalive Frames:  ▼

Country:  ▼

Max Station Count:  ▼

Multicast Helper:  ▼

HT Tx Chains:  ▼

HT Rx Chains:  ▼

HT Guard Interval:  ▼

OK  
Cancel  
Apply  
Comment  
Copy  
Remove



CAPsMAN

Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Ta

+ - 📄 🔍

Name	SSID	Hide SSID	Load Bal...	Country	Channel	Frequency	Band
cfg1	cap_test_localhost						2ghz-b/g/n

CAPs Configuration <cfg1>

Wireless **Channel** Rates Datapath Security

Channel:

Frequency:

Control Channel Width:

Band: 2ghz-b/g/n

Extension Channel:

Tx Power:

Save Selected:

Reselect Interval:

Skip DFS Channels:

OK  
Cancel  
Apply  
Comment  
Copy  
Remove

CAPsMAN

Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Ta

+ - 📁 📏

Name	SSID	Hide SSID	Load Bal...	Country	Channel	Frequency	Band
cfg1	cap_test_localhost						2ghz-b/g/n

CAPs Configuration <cfg1>

Wireless Channel Rates **Datapath** Security

Datapath:

MTU:

L2 MTU:

ARP:

Bridge:

Bridge Cost:

Bridge Horizon:

Local Forwarding:

Client To Client Forwarding:

VLAN Mode:

VLAN ID:

OK  
Cancel  
Apply  
Comment  
Copy  
Remove

CAPsMAN

Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Ta

+ - 📁 📏

Name	SSID	Hide SSID	Load Bal...	Country	Channel	Frequency	Band
cfg1	cap_test_localhost						2ghz-b/g/n

CAPs Configuration <cfg1>

Wireless Channel Rates Datapath **Security**

Security:

Authentication Type:  WPA PSK  WPA2 PSK  WPA EAP  WPA2 EAP

Encryption:  aes ccm  tkip

Group Encryption:

Group Key Update:

Passphrase:

EAP Methods:

EAP Radius Accounting:

TLS Mode:

TLS Certificate:

OK  
Cancel  
Apply  
Comment  
Copy  
Remove

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio

+ - ✓ ✗ 📁 🗑️

#	Radio MAC	Identity Reg...	Common Na...	Action	Master Configura...	Slave Configuration
0	00:00:00:00:00:00			create d...	cfg1	

CAPs Provisioning <00:00:00:00:00:00>

Radio MAC: 00:00:00:00:00:00

Hw. Supported Modes: gn

b

Identity Regexp:

Common Name Regexp:

IP Address Ranges:

Action: create dynamic enabled

Master Configuration: cfg1

Slave Configuration:

Name Format: cap

Name Prefix:

enabled

OK Cancel Apply Disable Comment Copy Remove

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio

+ - ✓ ✗ 📁 🗑️

#	Radio MAC	Identity Reg...	Common Na...	Action	Master Configura...	Slave Configuration
0	00:00:00:00:00:00			create d...	cfg1	

CAPs Provisioning <00:00:00:00:00:00>

Radio MAC: 00:00:00:00:00:00

Hw. Supported Modes: gn

b

Identity Regexp:

Common Name Regexp:

IP Address Ranges:

Action: create dynamic enabled

Master Configuration: cfg1

Slave Configuration:

Name Format: cap

Name Prefix:

enabled

OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove

# CAPsMAN

The screenshot displays the CAPsMAN configuration interface. The 'CAP Interface' tab is selected and highlighted with a red box. Below the tabs, a table lists the configured CAP interfaces:

Name	Type	MTU	Actual MTU	L2 MTU	Tx	Rx
cap1	CAP Interface	1500	1500	1600		0 bps

The 'Manager' button is also highlighted with a red box, and a red arrow points to the 'CAPs Manager' dialog box. The dialog box contains the following settings:

- Enabled
- Certificate: auto
- CA Certificate: auto
- Require Peer Certificate
- Generated Certificate: CAPsMAN-000C4200635C
- Generated CA Certificate: CAPsMAN-CA-000C4200635C
- Package Path: [Empty field]
- Upgrade Policy: none

Buttons for OK, Cancel, Apply, and Interfaces are visible on the right side of the dialog box.

# CAPsMAN

The screenshot displays the CAPsMAN web interface. At the top, there is a navigation menu with tabs: Provisioning, Configurations, Channels, Datapaths, Security Cfg., Access List, Rates, Remote CAP (highlighted with a red box), Radio, and Registration Ta. Below the menu are buttons for Provision, Upgrade, and Set Identity. A table lists the configuration details for a Remote CAP:

Address	Name	Board	Serial	Version	Identity	Base MAC	State
192.168.39.2	CAPsMAN-C...	RB751U-2HnD	2B3001DD3BEB	6.39rc80	Rb751-cap-test	00:0C:42:00:63:5C	Run

A dialog box titled "CAPs Remote AP <CAPsMAN-CA-000C4200635C>" is open, showing the configuration for the selected Remote AP. The fields are as follows:

- Address: 192.168.39.2
- Port: 44461
- Name: CAPsMAN-CA-000C4200635C
- Board: RB751U-2HnD
- Serial: 2B3001DD3BEB
- Version: 6.39rc80
- Identity: Rb751-cap-test
- Base MAC: 00:0C:42:00:63:5C
- State: Run
- Radios: 1

Buttons on the right side of the dialog include OK, Remove, Provision, Upgrade, and Set Identity. The bottom left of the dialog shows "1 item (1)".

# CAPsMAN

The screenshot displays the CAPsMAN interface with a table of CAPs and a detailed view of a selected CAP client. The table has columns for Interface, SSID, MAC Address, Tx Rate, Rx Rate, Tx Signal, Rx Signal, Uptime, and Tx/Rx Packets. The selected row is highlighted in blue. A red box highlights the 'Registration Ta' tab in the top menu, and another red box highlights the selected row in the table. A red arrow points from the 'Registration Ta' tab to the 'CAPs AP Client' dialog box.

Interface	SSID	MAC Address	Tx Rate	Rx Rate	Tx Signal	Rx Signal	Uptime	Tx/Rx Packets
cap1	cap_test_localhost	40:B8:37:D2:B6:42	104Mbps...	78Mbps...	0	-44	00:02:2...	42

**CAPs AP Client <40:B8:37:D2:B6:42>**

Interface: cap1

SSID: cap\_test\_localhost

MAC Address: 40:B8:37:D2:B6:42

Tx Rate: 104Mbps-20MHz/25

Rx Rate: 78Mbps-20MHz/25

Tx Rate Set: CCK:1-11 OFDM:6-54 BW:1x HT:0-15

Tx Signal: 0

Rx Signal: -44

Uptime: 00:02:26.39

Tx/Rx Packets: 423/498

Tx/Rx Bytes: 196.1 KIB/81.1 KIB

Buttons: OK, Remove, Copy to Access List



# CAPsMAN

- Possibility to provision different configurations on the same device (2GHz and 5GHz)
  - Create two configurations
  - Create two provisioning criteria (bgn, an or ac)
- Common config parameters can be set in templates (channel, datapath, security)

# 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!**