

Wireless AP and CAPsMAN Case Study

Uldis Cernevskis
MikroTik, Latvia

MUM Costa Rica

January 2016

Wireless AP features

- Provides wireless connectivity to Ethernet network resources
- Secure wireless communication using Pre-Shared-Key authentication and AES Encryption
- Wireless access limit by MAC address
- Centralized wireless client authentication using RADIUS

Wireless AP usage cases

- Apartments
- Residential buildings
- Offices
- Warehouses
- Coffee shops, Restaurants
- Museums, Theaters, Shopping centers
- Hotels
- Airports
- Government institutions
- Parks

Managing multiple AP's

- Time consuming new AP deployment due to the preconfiguring of the AP's
- Hard to adjust the configuration on all the AP's at the same time
- Hard to track the wireless clients connections among all the AP's

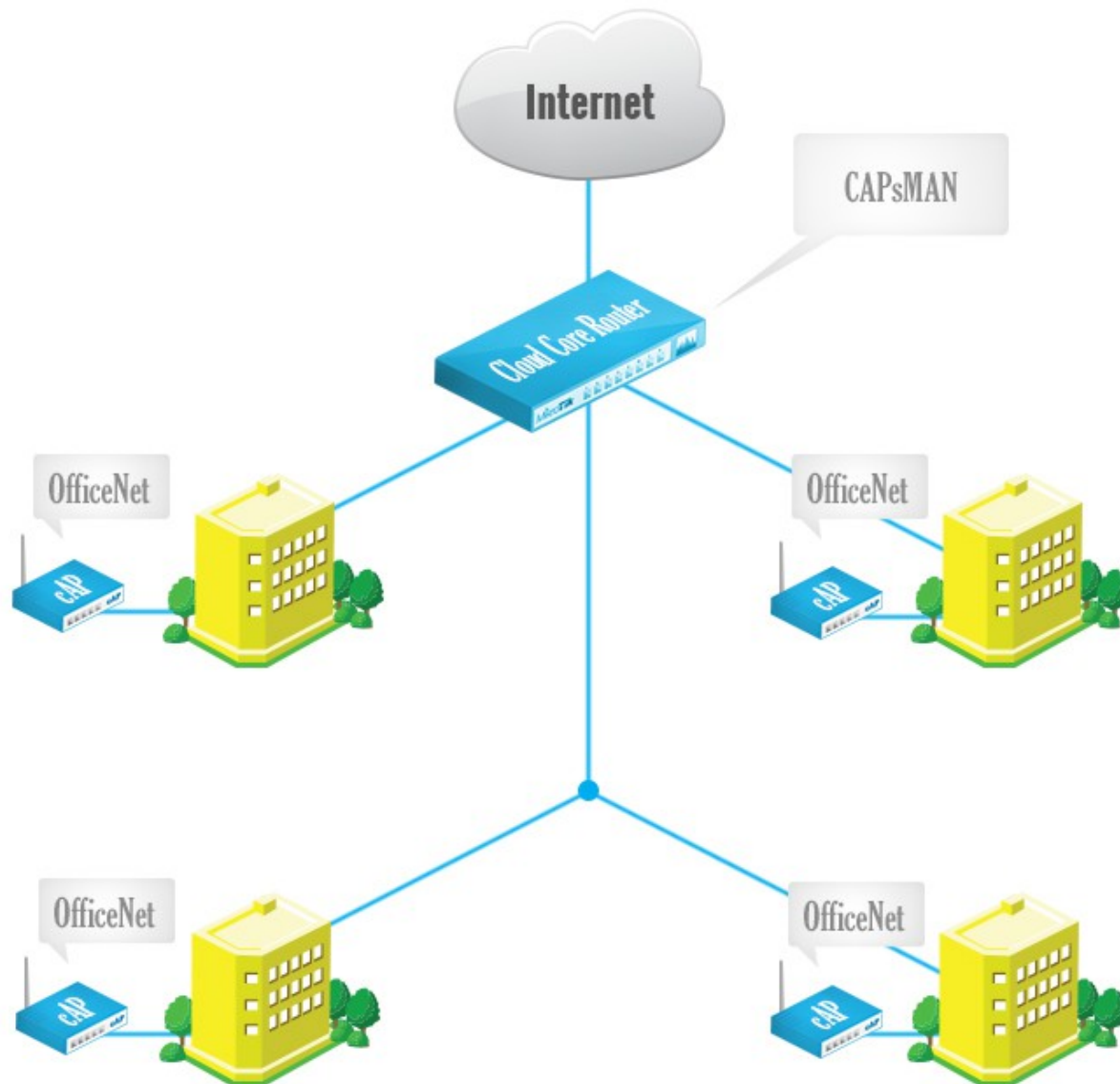
CAPsMAN Features

- Centralized management of RouterOS APs
- Dual Band AP support
- Provisioning of APs
- MAC and IP Layer communication with APs
- Certificate support for AP communication
- Full and Local data forwarding mode
- RADIUS MAC authentication
- Custom configuration support

Requirements

- CAPsMAN
 - x86, CHR and RouterBOARD based device
 - Newest RouterOS v6 version
 - Wireless-fp/cm2 package installed and enabled
- CAP
 - X86 or RouterBOARD based device
 - Newest RouterOS v6 version
 - Atheros chipset (a/b/g/n/ac) wireless card
 - Wireless-fp/cm2 package installed and enabled
 - At least Level4 RouterOS license

CAPsMAN Simple Setup

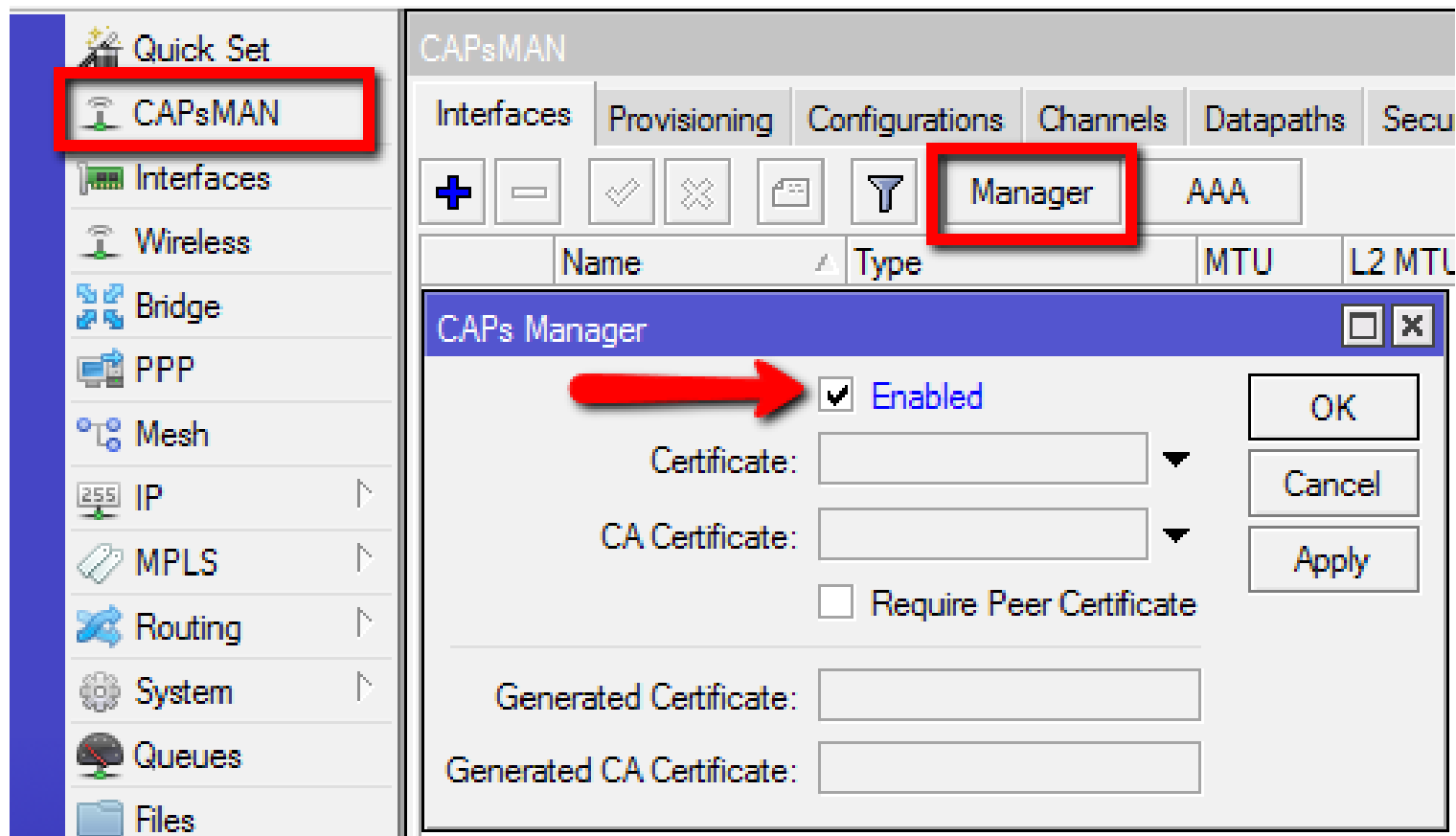


CAPsMAN Simple Setup

- Enable CAPsMAN service
- Create Bridge interface
- Add IP configuration to Bridge interface
- Create CAPsMAN Configuration
- Create Provisioning rule
- Enable CAP mode on the APs

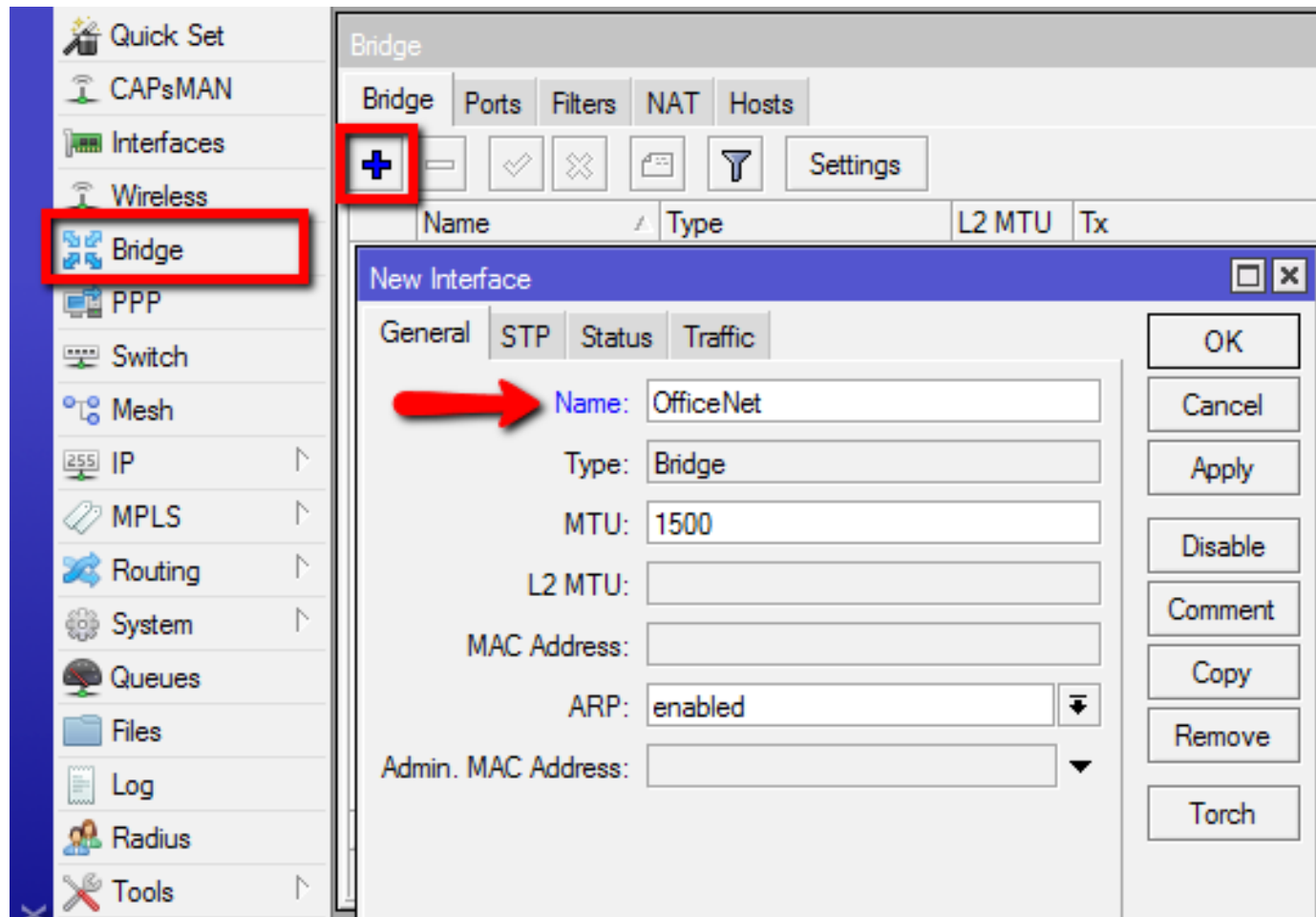
CAPsMAN Simple Setup

- Enable the CAPsMAN service



CAPsMAN Simple Setup

- Create Bridge Interface



CAPsMAN Simple Setup

- 1. Add IP address
- 2. Add DHCP Server
- 3. Add NAT rule

The screenshot displays the Mikrotik WinBox interface with three configuration windows open, each marked with a red box and a number:

- Address List:** A red box with the number '1' highlights the '+' icon in the top-left corner of the window, indicating the step to add a new address.
- DHCP Server:** A red box with the number '2' highlights the 'DHCP Setup' button in the top-right corner of the DHCP Server window.
- Firewall:** A red box with the number '3' highlights the 'NAT' tab in the Firewall window, indicating the step to add a new NAT rule.

The 'New Address' dialog shows the address '10.10.10.1/24' and interface 'OfficeNet'. The 'DHCP Setup' dialog shows the 'DHCP Server Interface' set to 'OfficeNet'. The 'New NAT Rule' dialog shows the chain 'srcnat' and action 'masquerade'.

CAPsMAN Simple Setup

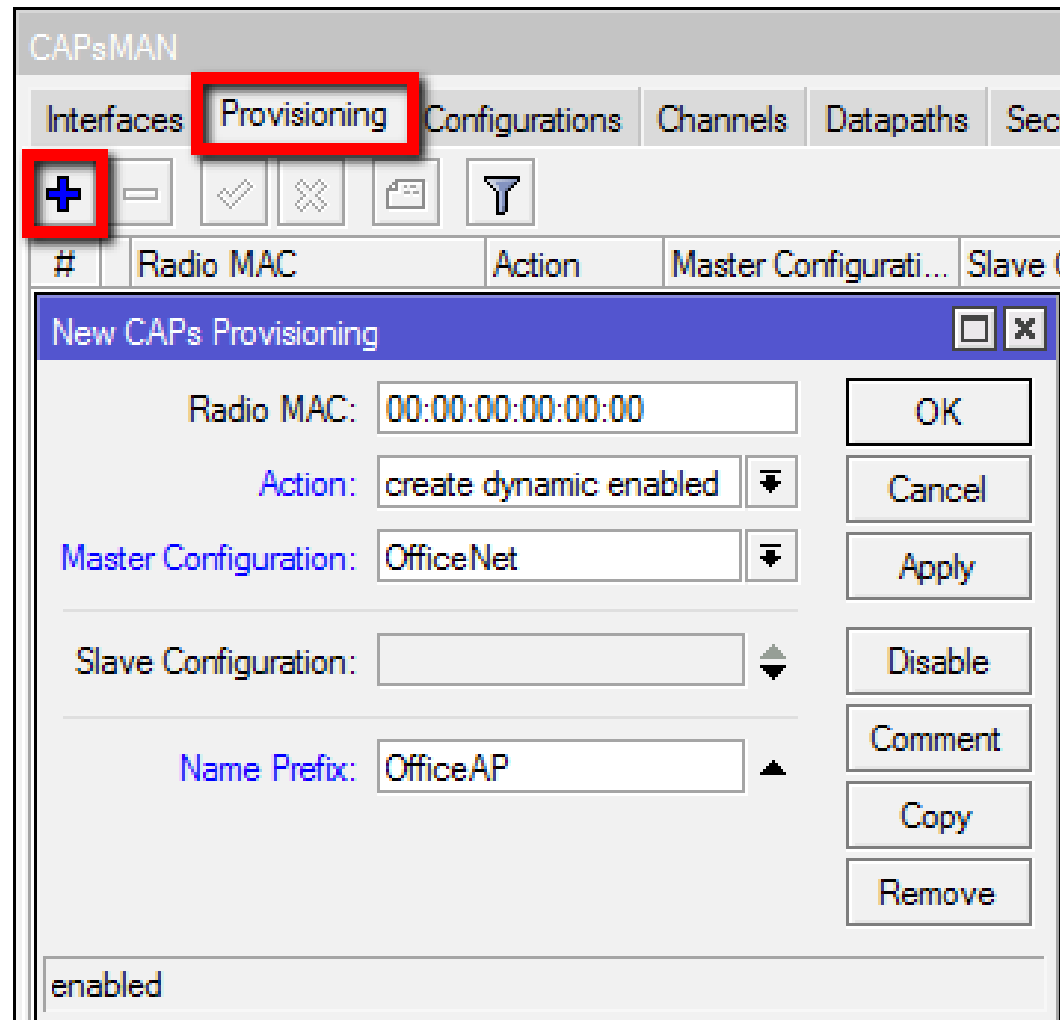
- Add New CAPsMAN Configuration

The screenshot displays the CAPsMAN configuration interface. At the top, the 'Configurations' tab is selected and highlighted with a red box. Below the tab, a toolbar contains a '+' icon (highlighted with a red box) and other navigation icons. A table header shows columns for Name, SSID, Hide SSID, Load Bal..., Country, Channel, Frequency, Band, and Datapat. Below the table, three configuration panels are visible, each with a red box around its tab:

- Wireless:** Name: OfficeNet, Mode: [empty], SSID: Office, Hide SSID: [empty], Load Balancing Group: [empty], Country: united states, Max Station Count: [empty], Multicast Helper: [empty], HT Tx Chains: [empty], HT Rx Chains: [empty], HT Guard Interval: [empty].
- Datapath:** Datapath: [empty], Bridge: OfficeNet, Bridge Cost: [empty], Bridge Horizon: [empty], Local Forwarding: [empty], Client To Client Forwarding: [empty], VLAN Mode: [empty], VLAN ID: [empty].
- Security:** Security: [empty], Authentication Type: WPA PSK WPA2 PSK WPA EAP WPA2 EAP, Encryption: aes ccm tkip, Group Encryption: aes ccm, Passphrase: OfficeNet, EAP Methods: [empty].

CAPsMAN Simple Setup

- Add new Provisioning rule



The screenshot shows the CAPsMAN interface with the 'Provisioning' tab selected. A red box highlights the '+' icon in the toolbar, indicating the action to add a new provisioning rule. The 'New CAPs Provisioning' dialog box is open, showing the following fields and options:

| # | Radio MAC | Action | Master Configurati... | Slave C |
|---|-------------------|------------------------|-----------------------|---------|
| | 00:00:00:00:00:00 | create dynamic enabled | OfficeNet | |

Dialog Box Fields:

- Radio MAC: 00:00:00:00:00:00
- Action: create dynamic enabled
- Master Configuration: OfficeNet
- Slave Configuration: (empty)
- Name Prefix: OfficeAP

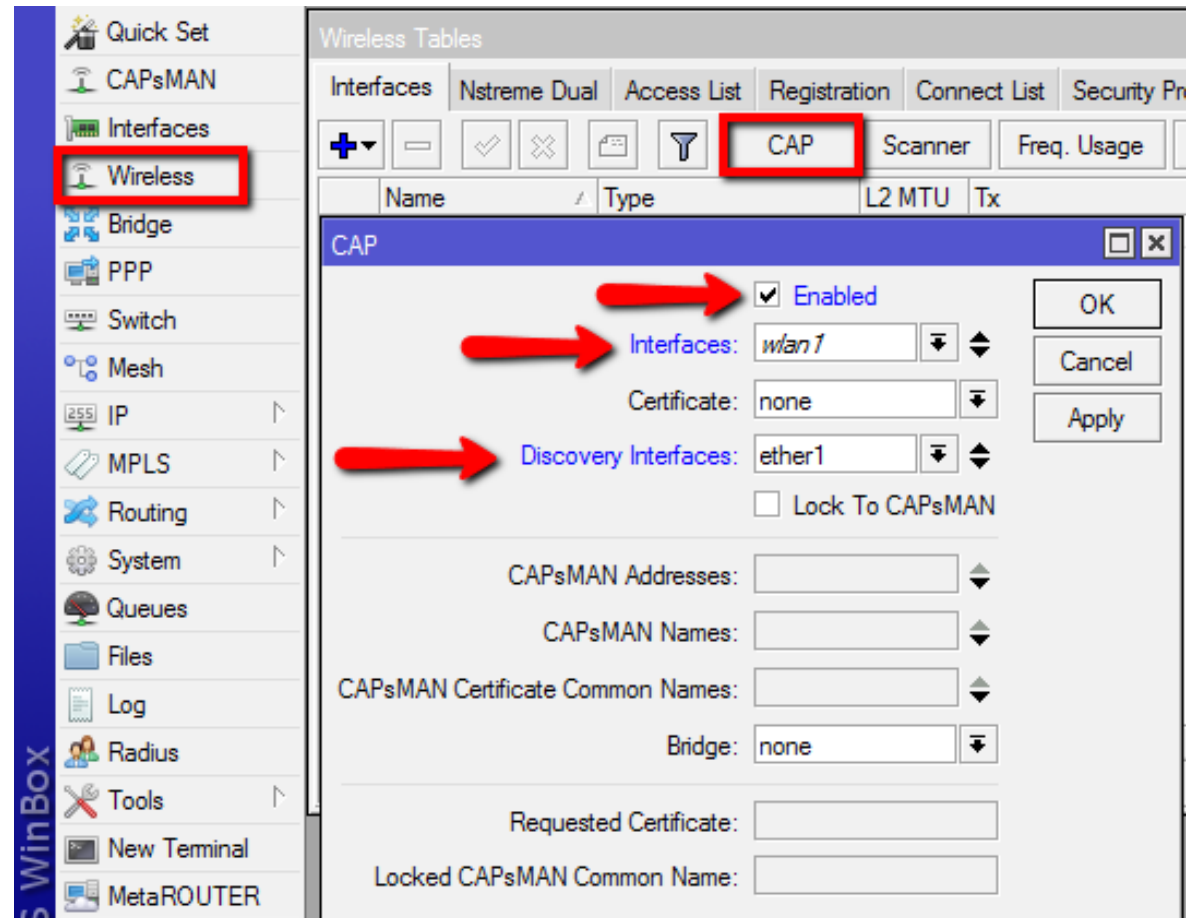
Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

enabled

CAPsMAN Simple Setup

- Configure the AP to use CAP mode

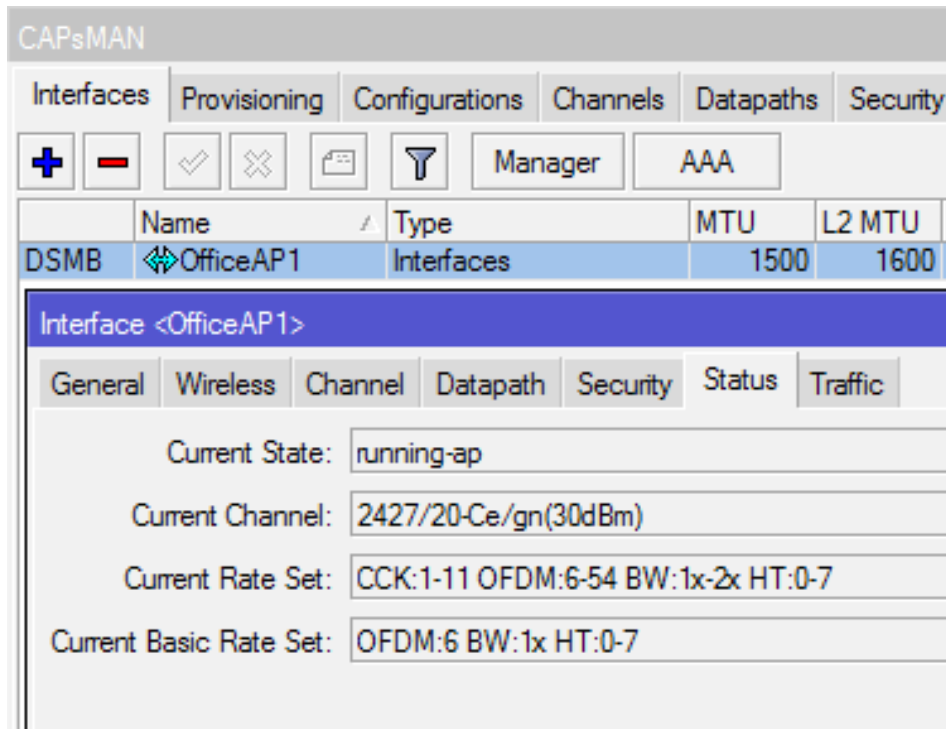
- Enable wireless-fp/cm2 package
- Enable CAP mode
 - By CAP mode button on some boards
 - By configuration in Wireless CAP menu



CAPsMAN Simple Setup

- Check the Status of the CAPsMAN CAP interface

CAPsMAN



The screenshot shows the CAPsMAN configuration interface. The 'Interfaces' tab is selected, displaying a table with columns: Name, Type, MTU, and L2 MTU. The interface 'OfficeAP1' is highlighted, showing its status as 'running-ap'.

| Name | Type | MTU | L2 MTU |
|----------------|------------|------|--------|
| DSMB OfficeAP1 | Interfaces | 1500 | 1600 |

Interface <OfficeAP1>

General | Wireless | Channel | Datapath | Security | Status | Traffic

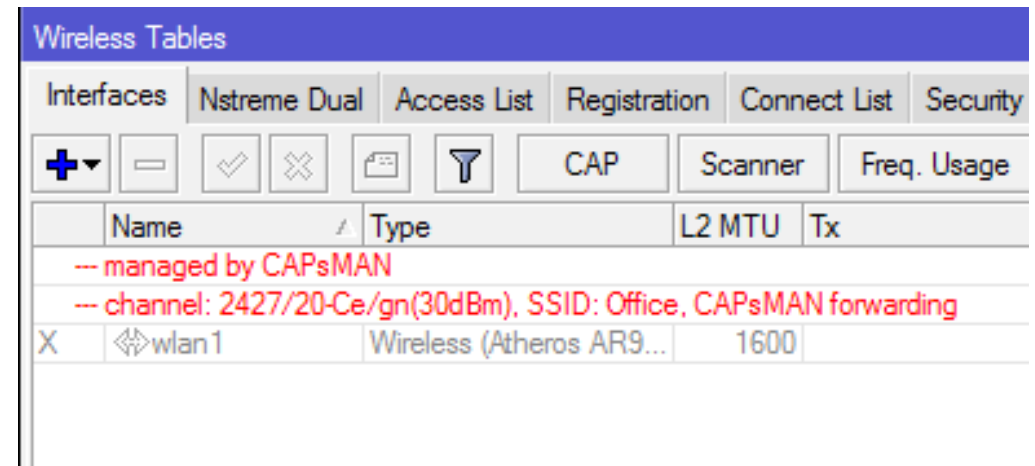
Current State: running-ap

Current Channel: 2427/20-Ce/gn(30dBm)

Current Rate Set: CCK:1-11 OFDM:6-54 BW:1x-2x HT:0-7

Current Basic Rate Set: OFDM:6 BW:1x HT:0-7

CAP



The screenshot shows the Wireless Tables configuration interface. The 'Interfaces' tab is selected, displaying a table with columns: Name, Type, L2 MTU, and Tx. The interface 'wlan1' is highlighted, showing its status as 'X' and its type as 'Wireless (Atheros AR9...)'.

| Name | Type | L2 MTU | Tx |
|---|--------------------------|--------|----|
| --- managed by CAPsMAN | | | |
| --- channel: 2427/20-Ce/gn(30dBm), SSID: Office, CAPsMAN forwarding | | | |
| X wlan1 | Wireless (Atheros AR9... | 1600 | |

CAPsMAN Registration table

CAPsMAN

Interfaces Provisioning Configurations Channels Datapaths Security Cfg. Access List Remote CAP Radio **Registration Table**

[-] [Filter]

| Interface | MAC Address | Tx Rate | Rx Rate | Tx Signal | Rx Signal | Uptime | Tx/Rx Packets | Tx/Rx Bytes |
|-----------|-------------------|------------|------------|-----------|-----------|-------------|---------------|-------------------|
| OfficeAP3 | 18:34:51:41:75:CD | 65Mbps-... | 65Mbps-... | 0 | -44 | 00:03:17... | 31 395/33 212 | 29.8 MiB/29.5 MiB |

1 item

CAPs AP Client <18:34:51:41:75:CD>

Interface: OfficeAP3

MAC Address: 18:34:51:41:75:CD

Tx Rate: 65Mbps-20MHz/1S

Rx Rate: 65Mbps-20MHz/1S

Tx Rate Set: CCK:1-11 OFDM:6-54 BW:1x HT:0-7

Tx Signal: 0

Rx Signal: -44

Uptime: 00:03:17.70

Tx/Rx Packets: 31 395/33 212

Tx/Rx Bytes: 29.8 MiB/29.5 MiB

OK

Remove

Copy to Access List

CAP to CAPsMAN Connection

- MAC Layer2:
 - No IP configuration required
 - CAP and CAPsMAN must be in the same Layer 2 network
- IP (UDP) Layer3:
 - CAP must reach the CAPsMAN using IP protocol
 - Can traverse NAT if necessary
- Management connection between CAP and CAPsMAN is secured using DTLS
- CAP client data traffic is not secured – if necessary additional encryption by using IPSec or encrypted tunnels is needed

CAPsMAN Selection on CAP

- CAP attempts to contact CAPsMAN and build available CAPsMAN list:
 - List of CAPsMAN IPs
 - List of CAPsMAN IPs obtained from DHCP
 - Broadcasting on configured interfaces using IP and MAC Layer
- CAP selects the CAPsMAN based on such rules:
 - If CAPsMAN names setting is matched it will prefer that CAPsMAN earlier in the list
 - MAC layer connectivity to CAPsMAN is preferred over IP connectivity
 - If list is empty it will connect to any available CAPsMAN

CAPsMAN with Layer3

- On the CAP specify the IP address of the CAPsMAN

Wireless Tables

Interfaces | Nstreme Dual | Access List | Registration | Connect List | Security Profiles | CAP

| Name | Type | L2 MTU | Tx | Rx |
|-------|--------------------------|--------|----|-------|
| wlan1 | Wireless (Atheros AR9... | 1600 | | 0 bps |

CAP

Enabled

Interfaces: wlan1

Certificate: none

Discovery Interfaces:

Lock To CAPsMAN

CAPsMAN Addresses: 10.5.125.1

CAPsMAN Names:

CAPsMAN Certificate Common Names:

Bridge: none

Requested Certificate:

Locked CAPsMAN Common Name:

OK
Cancel
Apply

CAPsMAN selection using Name

- On the CAP specify the CAPsMAN identity name

Wireless Tables

Interfaces | Nstreme Dual | Access List | Registration | Connect List | Security Profiles | CAP

+ | - | ✓ | ✗ | 📄 | 🗑️ | CAP | Scanner | Freq. Usage | Alignmer

| Name | Type | L2 MTU | Tx | Rx |
|------|------|--------|----|----|
| CAP | | | | |

CAP [Close] [X]

Enabled

Interfaces: [v] [^]

Certificate: [v]

Discovery Interfaces: [v] [^]

Lock To CAPsMAN

CAPsMAN Addresses:

CAPsMAN Names: [v] [^]

CAPsMAN Certificate Common Names:

Bridge: [v]

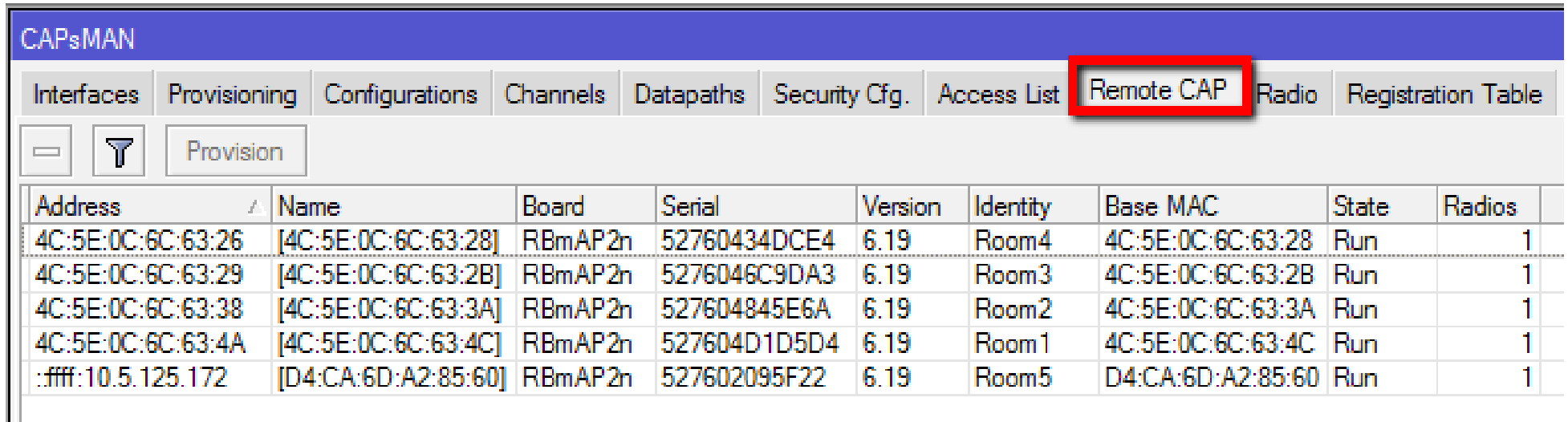
Requested Certificate:

Locked CAPsMAN Common Name:

OK
Cancel
Apply

CAP Identification

- MAC/IP address
- RouterBoard model
- Serial Number of the Board
- RouterOS version
- System Identity
- Main wireless MAC
- State of the CAP
- Provided radio count



The screenshot shows the Mikrotik CAPsMAN web interface. The 'Remote CAP' tab is selected and highlighted with a red box. Below the navigation tabs, there are buttons for 'Provision', a filter icon, and a minus sign. The main content area displays a table with the following columns: Address, Name, Board, Serial, Version, Identity, Base MAC, State, and Radios. The table contains five rows of data representing different Remote CAPs.

| Address | Name | Board | Serial | Version | Identity | Base MAC | State | Radios |
|-------------------|---------------------|---------|--------------|---------|----------|-------------------|-------|--------|
| 4C:5E:0C:6C:63:26 | [4C:5E:0C:6C:63:28] | RBmAP2n | 52760434DCE4 | 6.19 | Room4 | 4C:5E:0C:6C:63:28 | Run | 1 |
| 4C:5E:0C:6C:63:29 | [4C:5E:0C:6C:63:2B] | RBmAP2n | 5276046C9DA3 | 6.19 | Room3 | 4C:5E:0C:6C:63:2B | Run | 1 |
| 4C:5E:0C:6C:63:38 | [4C:5E:0C:6C:63:3A] | RBmAP2n | 527604845E6A | 6.19 | Room2 | 4C:5E:0C:6C:63:3A | Run | 1 |
| 4C:5E:0C:6C:63:4A | [4C:5E:0C:6C:63:4C] | RBmAP2n | 527604D1D5D4 | 6.19 | Room1 | 4C:5E:0C:6C:63:4C | Run | 1 |
| :fff:10.5.125.172 | [D4:CA:6D:A2:85:60] | RBmAP2n | 527602095F22 | 6.19 | Room5 | D4:CA:6D:A2:85:60 | Run | 1 |

CAPsMAN static CAP interface

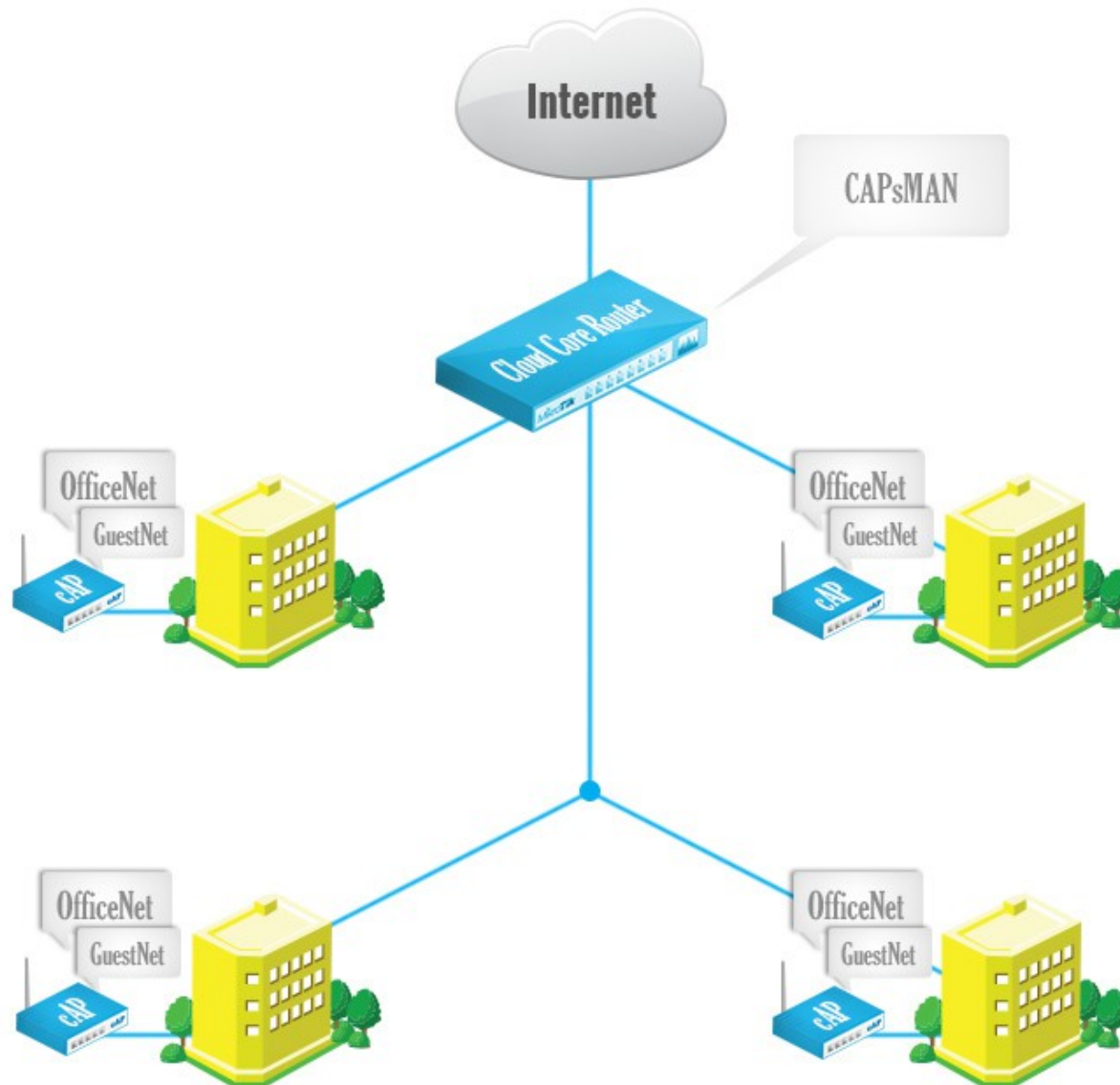
- No interface name change or setting change after the reboot
- Additional manual setting override
- Copy dynamic interface to make static interface

The screenshot displays the CAPsMAN configuration interface. At the top, there are tabs for 'Interfaces', 'Provisioning', 'Configurations', 'Channels', 'Datapaths', 'Security Cfg.', 'Access List', 'Remote CAP', 'Radio', and 'Registration Table'. Below these are icons for adding, deleting, and refreshing, along with a 'Manager' button and an 'AAA' dropdown menu. A table lists the current interfaces:

| Name | Type | MTU | L2 MTU | Tx | Rx | Tx Packet (p/s) | Rx Packet (p/s) | SSID | Hide SSID |
|-----------|------------|------|--------|-------|-------|-----------------|-----------------|--------|-----------|
| OfficeAP5 | Interfaces | 1500 | 1600 | 0 bps | 0 bps | 0 | 0 | Office | |

Below the table, the 'Interface <OfficeAP5>' configuration window is open, showing fields for Name, Type, MTU, L2 MTU, MAC Address, ARP, Radio MAC, and Master Interface. The 'Copy' button is highlighted with a red box. A red arrow points from this 'Copy' button to the 'New Interface' configuration window. In the 'New Interface' window, the 'Name' field is set to 'Room5AP', and the 'OK' button is also highlighted with a red box.

CAPsMAN VirtualAP



CAPsMAN VirtualAP Configuration

- Create new Bridge interface and IP configuration for the VirtualAPs or use the same bridge interface as Master AP
- Create a new configuration for the VirtualAP
- Specify the new configuration in Provisioning rule as Slave Configuration
- Remove all CAP interfaces
- Initiate Manual Provisioning on all the CAPs

CAPsMAN VirtualAP Setup

The screenshot displays the CAPsMAN configuration interface. At the top, a navigation bar includes tabs for 'Interfaces', 'Provisioning', 'Configurations', 'Channels', 'Datapaths', 'Security Cfg.', 'Access List', 'Remote CAP', 'Radio', and 'Registration Table'. The 'Configurations' tab is selected and highlighted with a red box. Below the navigation bar, a toolbar contains a plus sign icon (highlighted with a red box), a minus sign icon, a speech bubble icon, and a funnel icon. A table below the toolbar lists existing configurations with columns for Name, SSID, Hide SSID, Load Bal..., Country, Channel, Frequency, and Band. One entry is visible: 'OfficeNet' with SSID 'Office' and Country 'united sta...'. Below the table, two 'New CAPs Configuration' dialog boxes are shown. The left dialog has the 'Wireless' tab selected (highlighted with a red box) and contains fields for Name (GuestNet), Mode, SSID (Guest), Hide SSID, Load Balancing Group, Country, Max Station Count, Multicast Helper, HT Tx Chains, HT Rx Chains, and HT Guard Interval. The right dialog has the 'Datapath' tab selected (highlighted with a red box) and contains fields for Datapath, Bridge (GuestNet), Bridge Cost, Bridge Horizon, Local Forwarding, Client To Client Forwarding, VLAN Mode, and VLAN ID.

CAPsMAN VirtualAP Setup

CAPsMAN

Interfaces **Provisioning** Configurations Channels Datapaths Sec

0 00:00:00:00:00:00 create dy... OfficeNet

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

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

Action: create dynamic enabled Cancel

Master Configuration: OfficeNet Apply

Slave Configuration: GuestNet Disable

Name Prefix: OfficeAP Comment

Copy

Remove

enabled

CAPsMAN

Interfaces Provisioning Configurations Channels Datapaths

| | Name | Type | MTU | L |
|------|-------------|------------|------|---|
| DSMB | OfficeAP1 | Interfaces | 1500 | |
| DSB | OfficeAP1-1 | Interfaces | 1500 | |
| DSMB | OfficeAP2 | Interfaces | 1500 | |
| DSB | OfficeAP2-1 | Interfaces | 1500 | |
| DSMB | OfficeAP3 | Interfaces | 1500 | |
| DSB | OfficeAP3-1 | Interfaces | 1500 | |
| DSMB | OfficeAP4 | Interfaces | 1500 | |
| DSB | OfficeAP4-1 | Interfaces | 1500 | |
| SMB | Room5AP | Interfaces | 1500 | |

CAPsMAN

Interfaces Provisioning Configurations Channels Datapaths Security Cfg. Access List Remote CAP **Radio**

Provision

| | Radio MAC | Remote CAP Name | Remote CAP Iden... | Interface |
|---|-------------------|---------------------|--------------------|-----------|
| P | 4C:5E:0C:6C:63:28 | [4C:5E:0C:6C:63:... | Room4 | OfficeAP1 |
| P | 4C:5E:0C:6C:63:2B | [4C:5E:0C:6C:63:... | Room3 | OfficeAP3 |
| P | 4C:5E:0C:6C:63:3A | [4C:5E:0C:6C:63:... | Room2 | OfficeAP5 |
| P | 4C:5E:0C:6C:63:4C | [4C:5E:0C:6C:63:... | Room1 | OfficeAP2 |
| P | D4:CA:6D:A2:85:60 | [D4:CA:6D:A2:85:... | Room5 | Room5AP |

CAPsMAN Access List Features

- MAC Authentication
- Radius Query support
- MAC Mask support
- Signal Range
- Time
- Private Passphrase
- VLAN ID assignment

CAPsMAN Access List

- Allow Apple devices to connect
- Rest of the connections pass to the RADIUS

The screenshot displays the CAPsMAN configuration interface with the 'Access List' tab selected. A table below the tabs shows the configuration for two new access rules. The first rule has a MAC address of 18:34:51:00:00:00 and an 'accept' action. The second rule has an empty MAC address field and a 'query radius' action. Both rules are currently enabled.

| # | MAC Address | MAC Mask | Interface | Signal Ra... | Action | Client To Clie... | VLAN Mo... | VLAN ID |
|---|-------------------|-------------------|-----------|--------------|--------------|-------------------|------------|---------|
| | 18:34:51:00:00:00 | FF:FF:FF:00:00:00 | | | accept | | | |
| | | | | | query radius | | | |

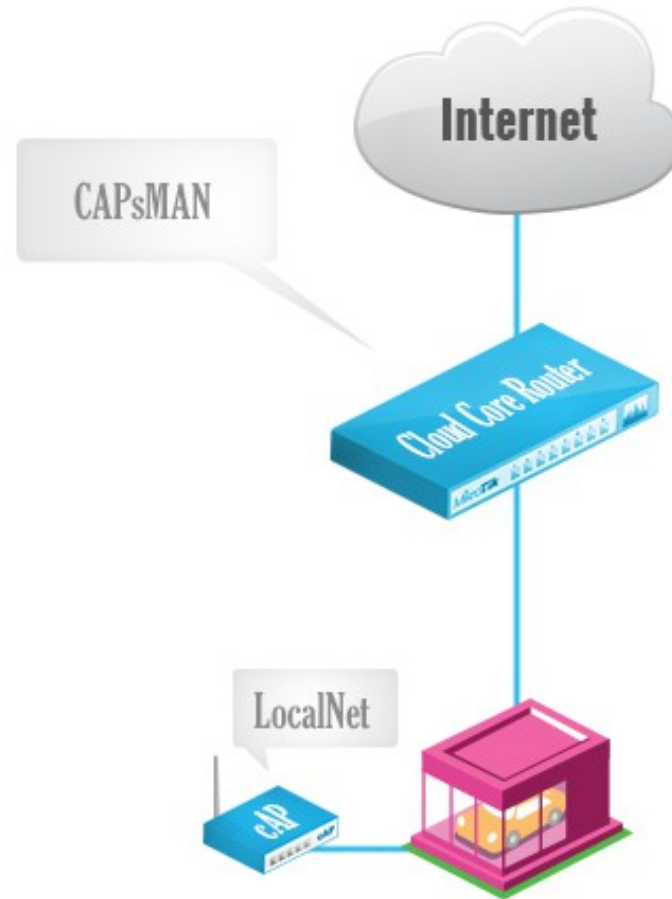
New CAPs Access Rule (Left Dialog):

- MAC Address: 18:34:51:00:00:00
- MAC Mask: FF:FF:FF:00:00:00
- Interface: [Empty]
- Signal Range: [Empty]
- Action: accept
- AP Tx Limit: [Empty]
- Client Tx Limit: [Empty]
- Private Passphrase: [Empty]
- Client To Client Forwarding: [Empty]
- RADIUS Accounting: [Empty]
- VLAN Mode: [Empty]
- VLAN ID: [Empty]
- Status: enabled

New CAPs Access Rule (Right Dialog):

- MAC Address: [Empty]
- MAC Mask: [Empty]
- Interface: [Empty]
- Signal Range: [Empty]
- Action: query radius
- AP Tx Limit: [Empty]
- Client Tx Limit: [Empty]
- Private Passphrase: [Empty]
- Client To Client Forwarding: [Empty]
- RADIUS Accounting: [Empty]
- VLAN Mode: [Empty]
- VLAN ID: [Empty]
- Status: enabled

CAPsMAN Local Forwarding Setup



CAPsMAN Local Forwarding

- Create a Local Forwarding configuration

The screenshot displays the CAPsMAN configuration interface. At the top, the 'Configurations' tab is selected and highlighted with a red box. Below the navigation tabs, a table lists existing configurations:

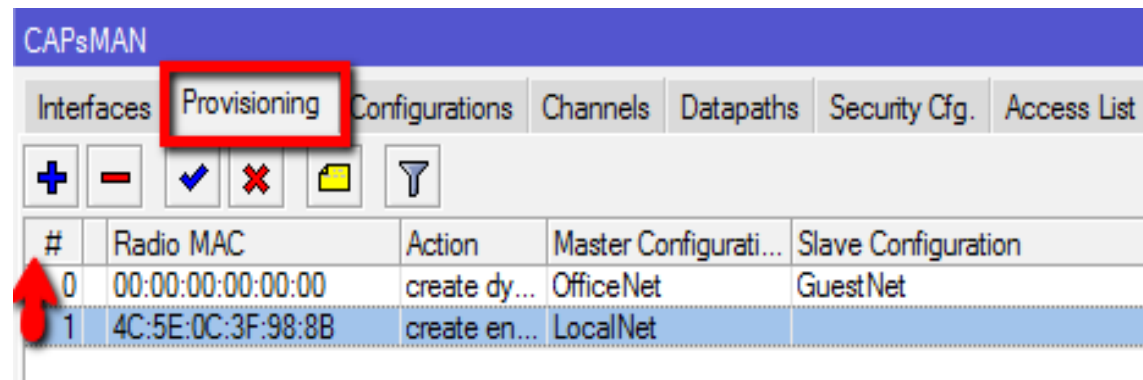
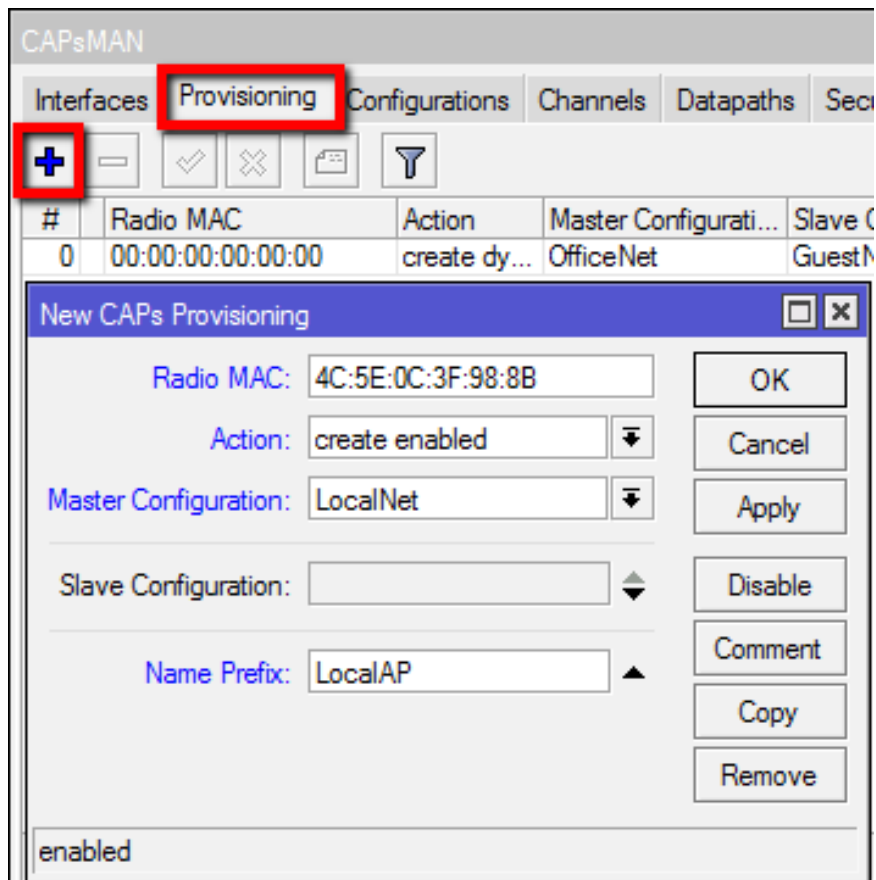
| Name | SSID | Hide SSID | Load Bal... | Country | Channel | Frequency | Band | Datapath | Bridge | VLAN M... |
|-----------|--------|-----------|-------------|---------------|---------|-----------|------|----------|-----------|-----------|
| GuestNet | Guest | | | | | | | | GuestNet | |
| OfficeNet | Office | | | united sta... | | | | | OfficeNet | |

Below the table, three configuration panels are shown for a new configuration named 'LocalNet':

- Wireless Panel:** The 'Wireless' tab is selected and highlighted with a red box. Fields include Name: LocalNet, Mode: (empty), SSID: LocalNet, Hide SSID: (empty), Load Balancing Group: (empty), Country: united states, Max Station Count: (empty), Multicast Helper: (empty), HT Tx Chains: (empty), HT Rx Chains: (empty), and HT Guard Interval: (empty).
- Datapath Panel:** The 'Datapath' tab is selected and highlighted with a red box. Fields include Datapath: (empty), Bridge: (empty), Bridge Cost: (empty), Bridge Horizon: (empty), Local Forwarding: , Client To Client Forwarding: (empty), VLAN Mode: (empty), and VLAN ID: (empty).
- Security Panel:** The 'Security' tab is selected and highlighted with a red box. Fields include Security: (empty dropdown), Authentication Type: WPA PSK WPA2 PSK WPA EAP WPA2 EAP, Encryption: aes ccm tkip, Group Encryption: aes ccm, Passphrase: LocalNet, and EAP Methods: (empty dropdown).

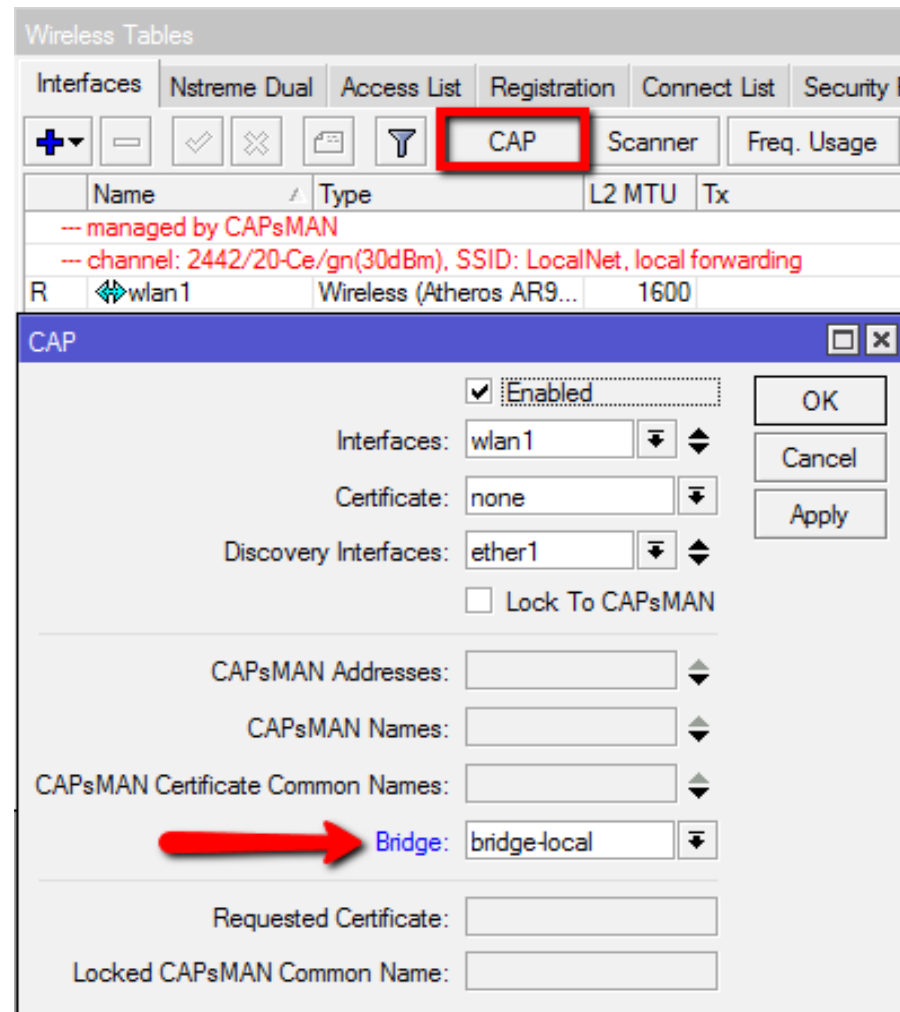
CAPsMAN Local Forwarding

- Create Provisioning rule
- Move above the default Provisioning rule



CAPsMAN Local Forwarding

- On CAP specify the Bridge interface for CAP or use routing for access to network



CAPsMAN Dual Band CAP

- If the Channel settings are not specified it will automatically use the supported band/channel
- If specific Channel settings are required then specific Provisioning rules are required
 - Custom Channel settings
 - Dual band wireless interface support

CAPsMAN Dual Band CAP

- Create 3 configurations:
 - Config for both bands radio
 - Config for 5ghz only radio
 - Config for 2.4ghz only radio

The screenshot shows the CAPsMAN web interface with the 'Configurations' tab selected. The interface is divided into three panels, each representing a different CAP configuration. The 'Channel' tab is highlighted in red in each panel. The first panel is for 'Both Bands', the second for '5ghz Config', and the third for '2.4ghz Config'. Each panel has a 'Wireless' sub-tab and a 'Channel' sub-tab. The 'Channel' sub-tab is active in each panel, showing fields for Channel, Frequency, Width, Band, Extension Channel, and Tx. Power.

| Name | SSID | Hide SSID | Load Bal... | Country | Channel | Frequency | Band | | | | |
|---------------------------------|----------|----------------------------------|-------------|------------------------------------|----------|-----------|----------|--------------------|------------|----------|----------|
| CAPs Configuration <Both Bands> | | CAPs Configuration <5ghz Config> | | CAPs Configuration <2.4ghz Config> | | | | | | | |
| Wireless | Channel | Datapath | Security | Wireless | Channel | Datapath | Security | Wireless | Channel | Datapath | Security |
| Channel: | | | | Channel: | | | | Channel: | | | |
| Frequency: | | | | Frequency: | | | | Frequency: | | | |
| Width: | 20 | | | Width: | 20 | | | Width: | | | |
| Band: | 5ghz-a/n | | | Band: | 5ghz-a/n | | | Band: | 2ghz-b/g/n | | |
| Extension Channel: | | | | Extension Channel: | | | | Extension Channel: | | | |
| Tx. Power: | | | | Tx. Power: | | | | Tx. Power: | | | |

CAPsMAN Dual Band CAP

- Create 3 Provisioning rules
 - For A/N,G/N hardware use Both Bands config
 - For A/N hardware use 5ghz config
 - For G/N hardware use 2.4ghz config

The screenshot shows the CAPsMAN web interface with the 'Provisioning' tab selected. The interface includes a navigation bar with tabs for 'Interfaces', 'Provisioning', 'Configurations', 'Channels', 'Datapaths', 'Security Cfg.', 'Access List', 'Remote CAP', 'Radio', and 'Registration Table'. Below the navigation bar is a toolbar with icons for adding, deleting, and filtering. The main content area displays three provisioning rule configurations, each with a 'Radio MAC' field set to '00:00:00:00:00:00' and an 'Action' of 'create dynamic enabled'. The first rule is for 'Both Bands' hardware, the second for '5ghz Config', and the third for '2.4ghz Config'. Each rule also has a 'Master Configuration' field and a 'Slave Configuration' field.

| # | Radio MAC | Action | Master Configurati... | Slave Configuration |
|---|-------------------|------------------------|-----------------------|---------------------|
| | 00:00:00:00:00:00 | create dynamic enabled | Both Bands | |
| | 00:00:00:00:00:00 | create dynamic enabled | 5ghz Config | |
| | 00:00:00:00:00:00 | create dynamic enabled | 2.4ghz Config | |

CAPsMAN Dual Band CAP

CAPsMAN

Interfaces Provisioning Configurations Channels Datapaths Security Cfg. Access List Remote CAP Radio Registr

+ - ✓ ✗ ☰ ⏏ Manager AAA

| Name | Type | MTU | L2 MTU | Tx | Rx |
|-------|------------|------|--------|-------|-------|
| cap10 | Interfaces | 1500 | 1600 | 0 bps | 0 bps |
| cap9 | Interfaces | 1500 | 1600 | 0 bps | 0 bps |

Interface <cap9>

General Wireless Channel Datapath Security

Configuration: 2.4ghz Config

Mode:

SSID: 2.4ghz band

Hide SSID:

Interface <cap10>

General Wireless Channel Datapath Security Status Traffic

Configuration: 5ghz Config

Mode:

SSID: 5ghz band

Hide SSID:

Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles Channels

+ - ✓ ✗ ☰ ⏏ CAP Scanner Freq. Usage Alignment Wireless Sniffer

| Name | Type | L2 MTU | Tx | Rx | Tx |
|---|--------------------------|--------|----|-------|-------|
| -- managed by CAPsMAN | | | | | |
| -- channel: 5220/20-Ce/an(17dBm), SSID: 5ghz band, CAPsMAN forwarding | | | | | |
| X wlan1 | Wireless (Atheros AR9... | 1600 | | 0 bps | 0 bps |
| -- managed by CAPsMAN | | | | | |
| -- channel: 2427/20-Ce/gn(30dBm), SSID: 2.4ghz band, CAPsMAN forwarding | | | | | |
| X wlan2 | Wireless (Atheros AR9... | 1600 | | 0 bps | 0 bps |

CAPsMAN Configuration override

- Configuration overrides Channel setting
- Interface overrides Channel and Configuration setting



New CAPs Channel

Name:

Frequency: MHz ▲

Width:

OK

Cancel

Apply

New CAPs Configuration

Wireless Channel Datapath Security

Channel:

Frequency: MHz ▲

Width:

New Interface

General Wireless Channel Datapath Security Status Traffic

Channel:

Frequency: MHz ▲

Width:

Interface <cap1>

General Wireless Channel Datapath Security Status Traffic

Current State:

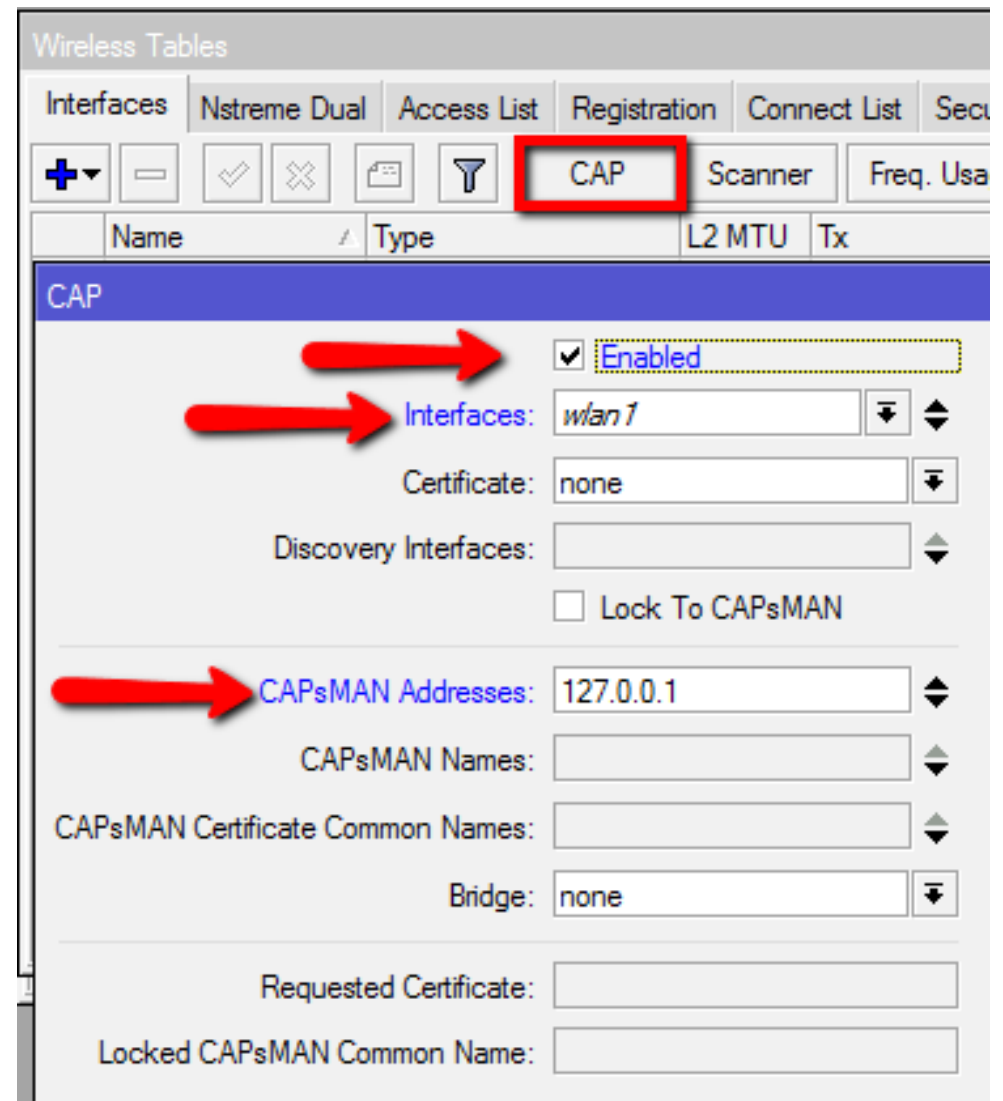
Current Channel:

Current Rate Set:

Current Basic Rate Set:

CAPsMAN and CAP in one board

- Enable CAPsMAN Manager and create the configuration
- Configure the CAP to look for IP 127.0.0.1



The screenshot shows the Mikrotik WinBox configuration interface for a CAP (Client Access Point) under the 'Wireless Tables' section. The 'CAP' tab is selected and highlighted with a red box. The configuration is for a CAP named 'CAP'. The 'Enabled' checkbox is checked, and the 'Interfaces' field is set to 'wlan1'. The 'CAPsMAN Addresses' field is set to '127.0.0.1'. Red arrows point to the 'Enabled' checkbox, the 'Interfaces' field, and the 'CAPsMAN Addresses' field. Other fields include 'Certificate: none', 'Discovery Interfaces', 'Lock To CAPsMAN' (unchecked), 'CAPsMAN Names', 'CAPsMAN Certificate Common Names', 'Bridge: none', 'Requested Certificate', and 'Locked CAPsMAN Common Name'.

| Name | Type | L2 MTU | Tx |
|------|------|--------|----|
| CAP | | | |

Wireless Tables

Interfaces | Nstreme Dual | Access List | Registration | Connect List | Secu

+ - ✓ ✗ [CAP] Scanner Freq. Usa

Enabled

Interfaces: wlan1

Certificate: none

Discovery Interfaces:

Lock To CAPsMAN

CAPsMAN Addresses: 127.0.0.1

CAPsMAN Names:

CAPsMAN Certificate Common Names:

Bridge: none

Requested Certificate:

Locked CAPsMAN Common Name:

CAPsMAN Antenna-gain

- Antenna-gain value is taken from the CAP interface
- Must be configured on AP before enable radio in CAP mode
- Example with 6db antenna-gain and 30db EIRP

The screenshot displays the CAPsMAN configuration interface. The top section shows a table of interfaces:

| Name | Type | MTU | L2 MTU | Tx |
|------|------------|------|--------|----|
| cap1 | Interfaces | 1500 | 1600 | |

Below this, the 'Wireless Tables' section shows a table of wireless interfaces:

| Name | Type | L2 MTU | Tx | Rx |
|------|--|--------|----|----|
| --- | managed by CAPsMAN | | | |
| --- | channel: 2442/20-Ce/gn(24dBm), SSID: LocalAP, CAPsMAN forwarding | | | |

The 'Interface <cap1>' configuration is shown below, with the 'Wireless' tab selected. The 'Current Channel' field is highlighted with a red box and contains the value '2442/20-Ce/gn(30dBm)'. Other fields include 'Current State: running-ap', 'Current Rate Set: CCK:1-11 OFDM:6-54 BW:1x-2x HT:0-15', and 'Current Basic Rate Set: OFDM:6 BW:1x HT:0-7'.

CAPsMAN v2 features

- CAPsMAN automatic upgrade of all CAP clients (configurable)
- Improved CAP<->CAPsMAN data connection protocol
- Added "Name Format, Name Prefix Identity/CommonName Regexp, IP Address Ranges" setting for Provision rules
- Improved logging entries when client roams between the CAPs
- Added L2 Path MTU discovery

CAPsMAN v2 compatibility

- CAPsMAN v2 is NOT compatible with current CAPsMAN v1 (CAPsMAN v1 CAP devices will not be able to connect to CAPsMAN v2 and CAPsMAN v2 CAP devices will not be able to connect to CAPsMAN v1).
- Both CAPsMAN and CAP devices should have wireless-cm2 package installed in order to make CAPsMAN v2 system to work.

Upgrade to CAPsMAN v2

- Option1: Install a new temporary CAPsMAN v2 router in same network where the current CAPsMAN router is and start upgrading CAPs with wireless-cm2 package. All CAPs with the v2 will connect to the new temporary CAPsMAN v2 router. After every CAP is upgraded to v2, upgrade your current CAPsMAN to v2 and then turn off the temporary CAPsMAN v2 router.
- Option2: Upgrade your CAPs and then CAPsMAN to v2 at the same time. In this case you could have little more downtime unless you schedule all the CAPs to reboot/install at the same time.