

Wireless AP and CAPsMAN Case Study

Uldis Cernevskis
MikroTik, Latvia

MUM Cuba

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

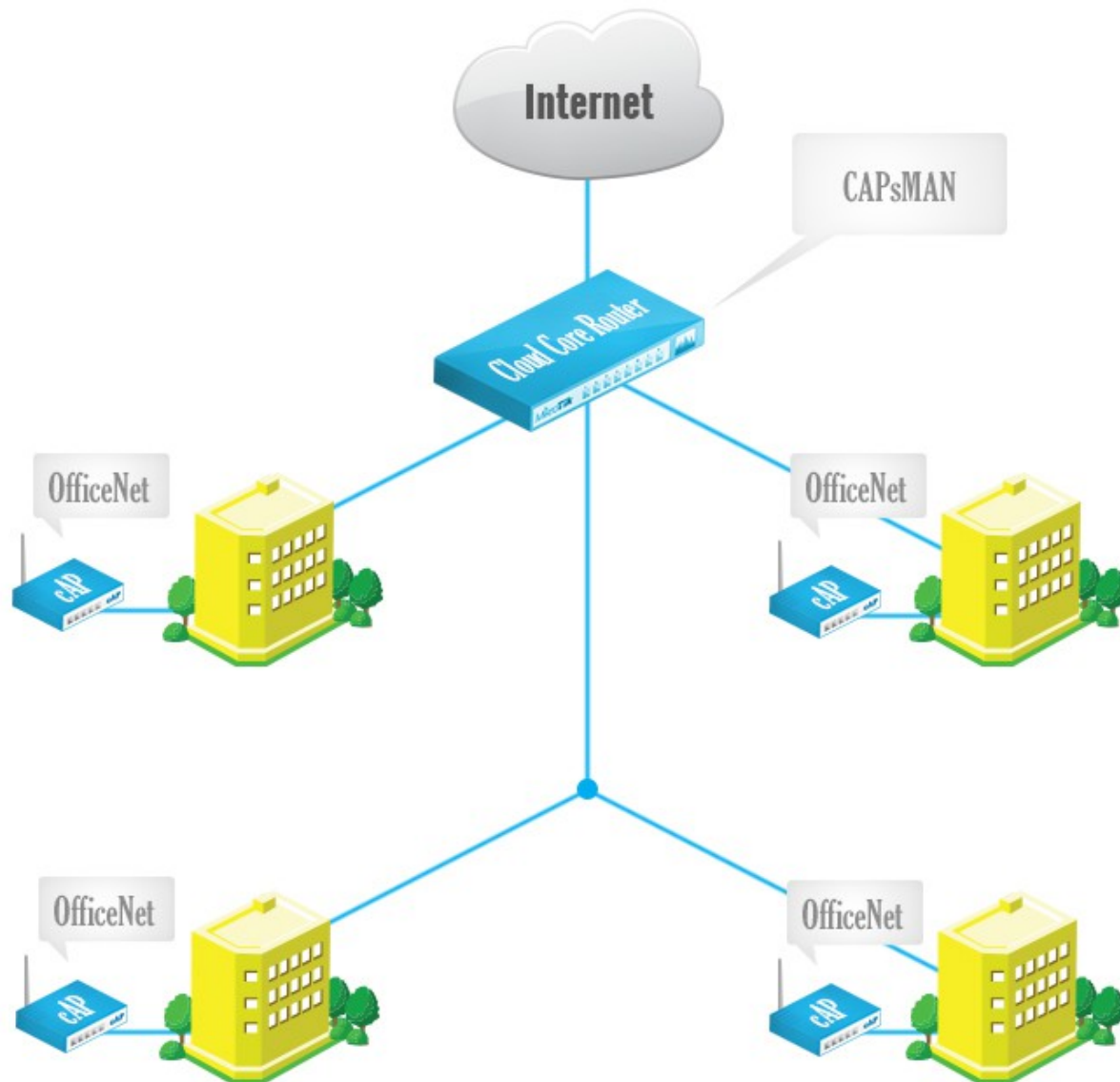
Requirements

- 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

CHR image on USB Flashdrive

- CHR RouterOS image in the USB drive
- Follow the instructions for installation on the USB Flashdrive to test RouterOS features
- Email support@mikrotik.com for any questions on the CHR usage

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

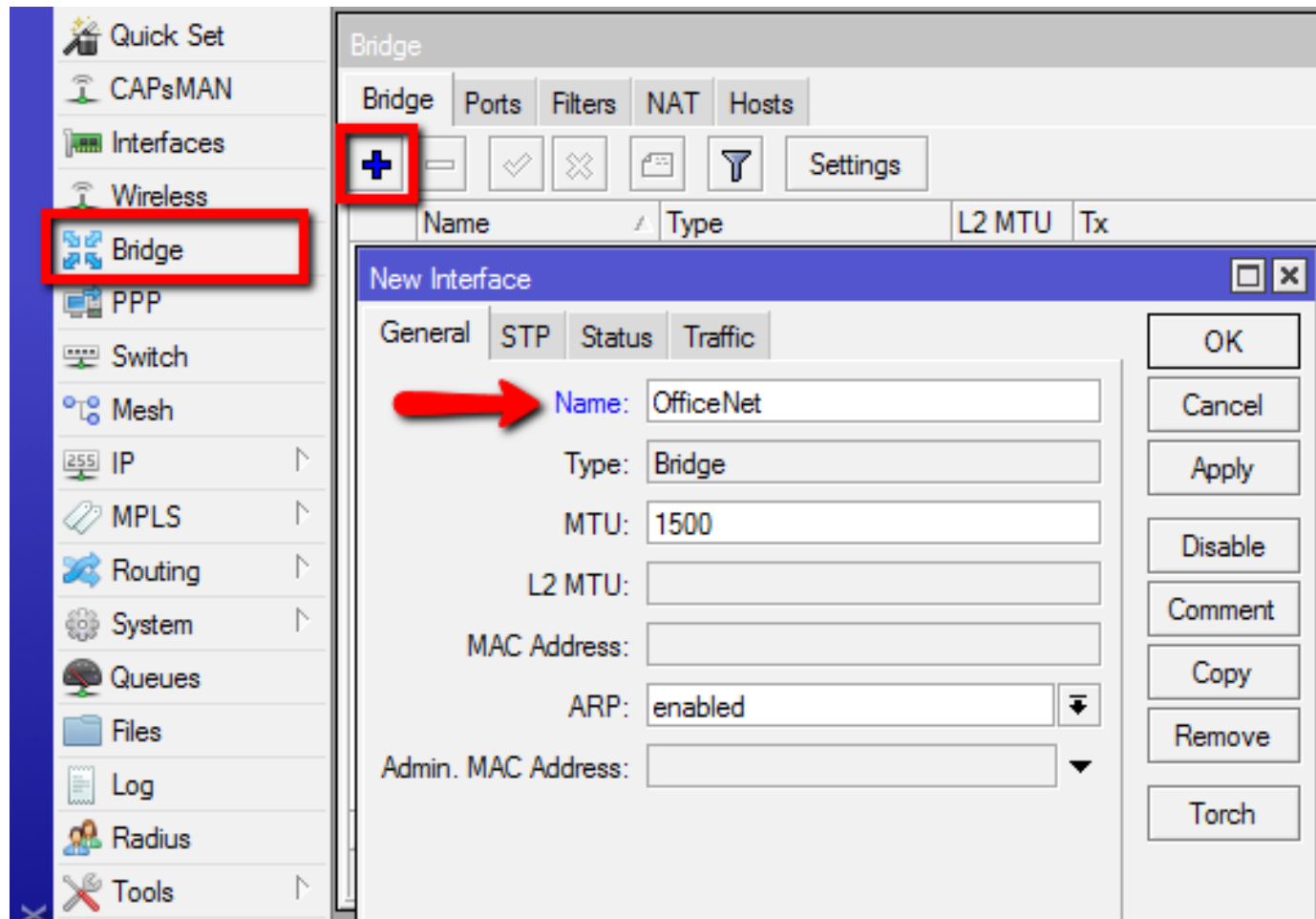
CAPsMAN Simple Setup

- Enable the CAPsMAN service

The screenshot displays the Mikrotik WinBox interface for configuring CAPsMAN. On the left sidebar, the 'CAPsMAN' menu item is highlighted with a red box. The main window shows the 'CAPsMAN' configuration page with several tabs: 'Interfaces', 'Provisioning', 'Configurations', 'Channels', 'Datapaths', and 'Security'. The 'Manager' tab is selected and highlighted with a red box. Below the tabs, there is a table with columns for 'Name', 'Type', 'MTU', and 'L2 MTU'. A red arrow points to the 'Enabled' checkbox, which is checked. Other fields include 'Certificate', 'CA Certificate', 'Require Peer Certificate', 'Generated Certificate', and 'Generated CA Certificate'. Buttons for 'OK', 'Cancel', and 'Apply' are visible on the right side of the configuration window.

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 windows open, each illustrating a step in the CAPsMAN setup process:

- Address List:** A window titled "Address List" with a toolbar containing a plus sign (+) and a minus sign (-). A red box labeled "1" highlights the plus sign. Below the toolbar, a "New Address" dialog is open, showing "Address: 10.10.10.1/24" and "Interface: OfficeNet".
- DHCP Server:** A window titled "DHCP Server" with tabs for "DHCP", "Networks", "Leases", "Options", "Option Sets", and "Alerts". A red box labeled "2" highlights the "DHCP Setup" button in the top right. Below, a "DHCP Setup" dialog is open, showing "DHCP Server Interface: OfficeNet" and a "Next" button highlighted with a red box.
- Firewall:** A window titled "Firewall" with tabs for "Filter Rules", "NAT", "Mangle", "Service Ports", "Connections", "Address Lists", and "Layer7 Protocols". A red box labeled "3" highlights the "NAT" tab. Below, a "New NAT Rule" dialog is open, showing "Chain: srcnat" and "Action: masquerade".

CAPsMAN Simple Setup

- Add New CAPsMAN Configuration

The screenshot displays the CAPsMAN configuration interface. The 'Configurations' tab is selected and highlighted with a red box. A red box also highlights the '+' icon in the toolbar. Below the toolbar, a table lists configurations with columns for Name, SSID, Hide SSID, Load Bal..., Country, Channel, Frequency, Band, and Datapat. Three configuration panels are shown below the table, each with a red box highlighting a specific tab: 'Wireless', 'Datapath', and 'Security'.

Configurations Tab:

Name	SSID	Hide SSID	Load Bal...	Country	Channel	Frequency	Band	Datapat
------	------	-----------	-------------	---------	---------	-----------	------	---------

Wireless Configuration Panel:

- Name: OfficeNet
- Mode: []
- SSID: Office
- Hide SSID: []
- Load Balancing Group: []
- Country: united states
- Max Station Count: []
- Multicast Helper: []
- HT Tx Chains: []
- HT Rx Chains: []
- HT Guard Interval: []

Datapath Configuration Panel:

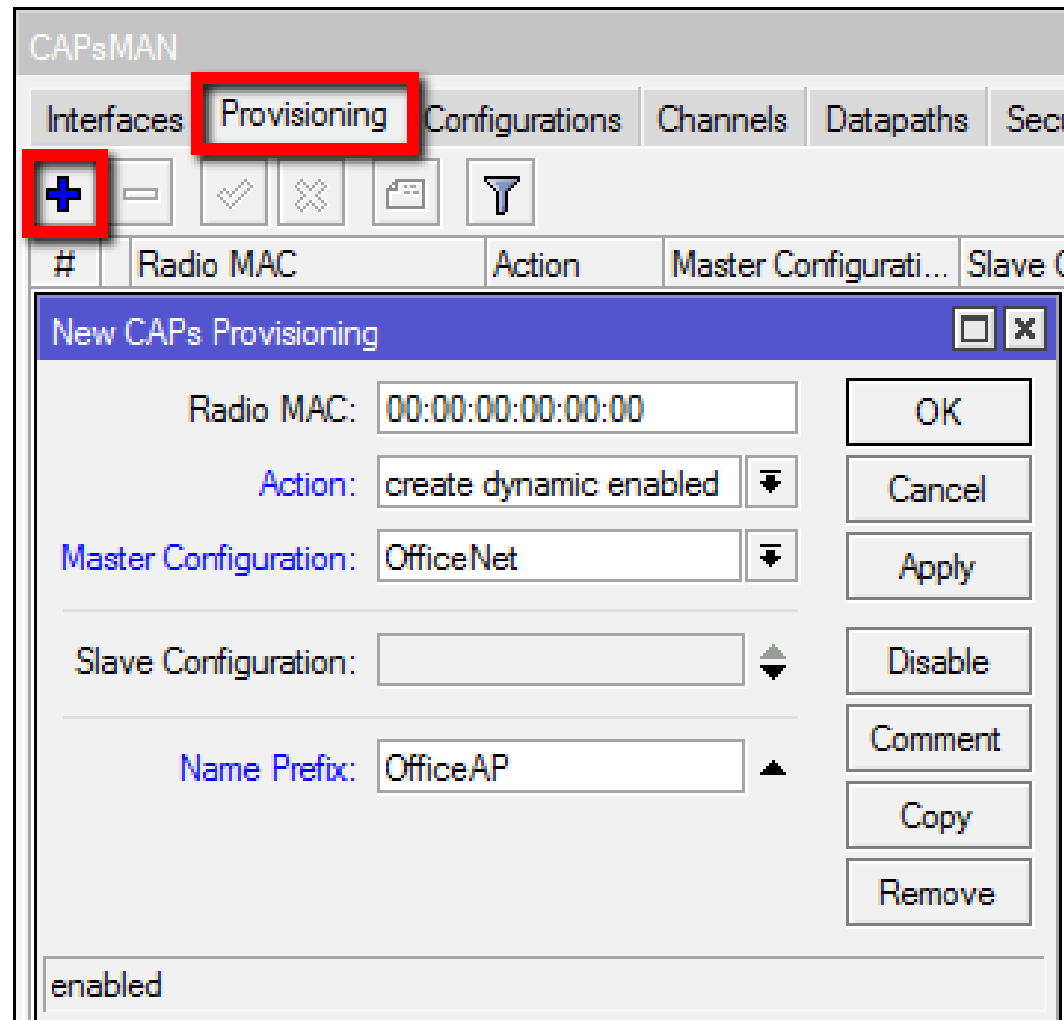
- Datapath: []
- Bridge: OfficeNet
- Bridge Cost: []
- Bridge Horizon: []
- Local Forwarding: []
- Client To Client Forwarding: []
- VLAN Mode: []
- VLAN ID: []

Security Configuration Panel:

- Security: []
- Authentication Type: WPA PSK WPA2 PSK WPA EAP WPA2 EAP
- Encryption: aes ccm tkip
- Group Encryption: aes ccm
- Passphrase: OfficeNet
- EAP Methods: []

CAPsMAN Simple Setup

- Add new Provisioning rule



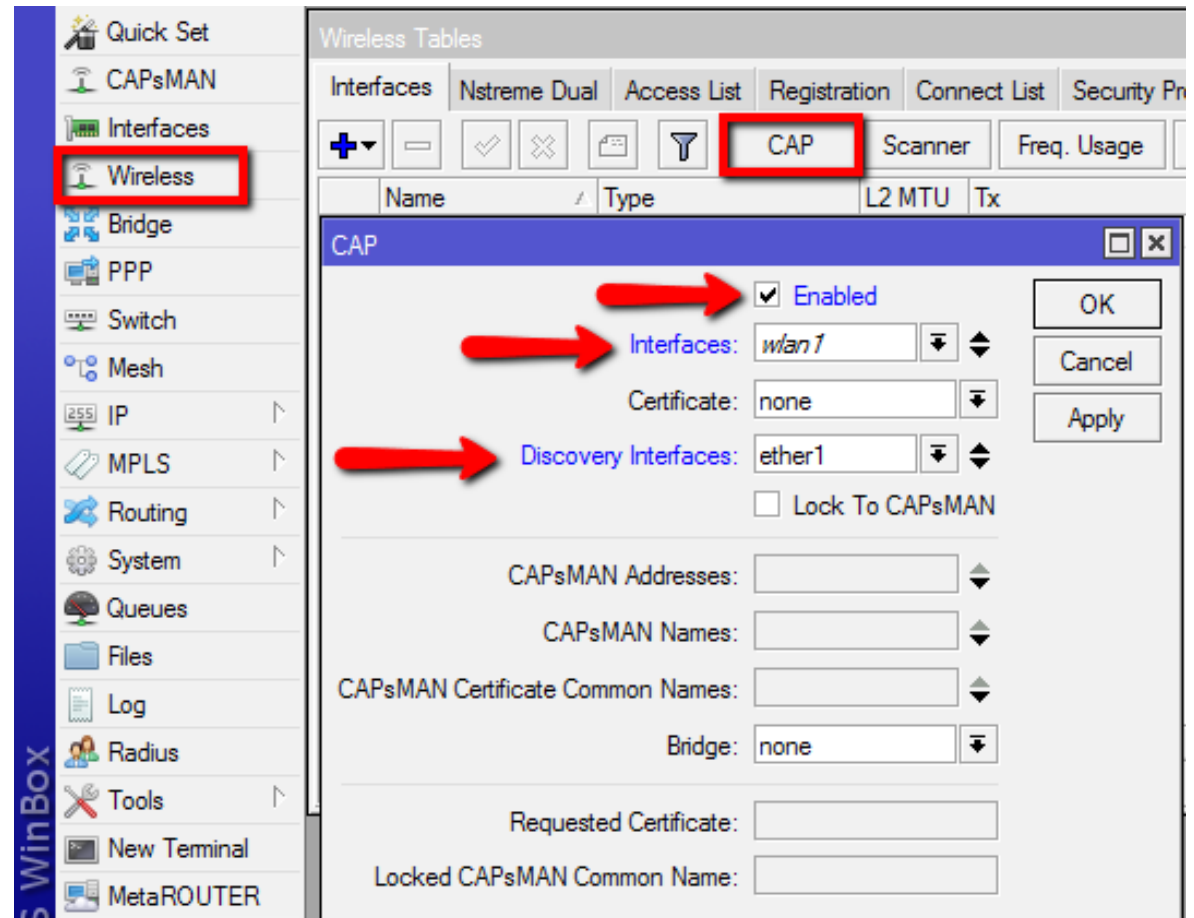
The screenshot shows the CAPsMAN software interface. The 'Provisioning' tab is selected and highlighted with a red box. Below the tab, a toolbar contains several icons, with a plus sign icon also highlighted by a red box. A dialog box titled 'New CAPs Provisioning' is open, showing the following fields and options:

#	Radio MAC	Action	Master Configurati...	Slave C
	Radio MAC: 00:00:00:00:00:00	Action: create dynamic enabled	Master Configuration: OfficeNet	Slave Configuration:
			Name Prefix: OfficeAP	

Buttons on the right side of the dialog box include: OK, Cancel, Apply, Disable, Comment, Copy, and Remove. The status 'enabled' is shown at the bottom left of the dialog box.

CAPsMAN Simple Setup

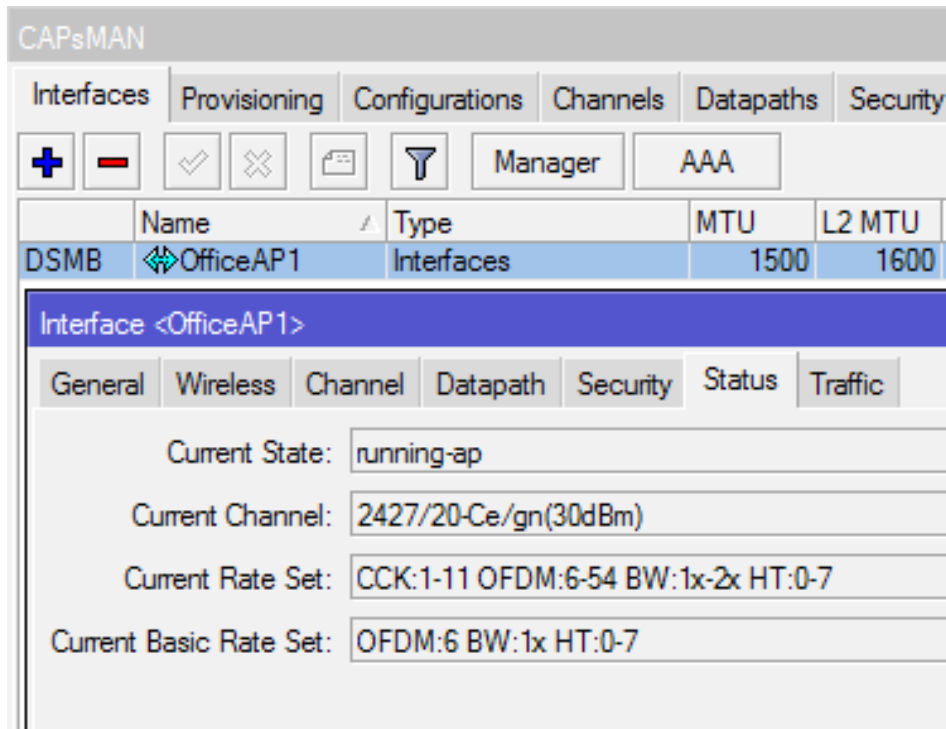
- Configure the AP to use CAP mode
 - Enable wireless-fp package
 - Enable CAP mode
 - By CAP mode button on some boards
 - By configuration in Wireless CAP menu



CAPsMAN Simple Setup

- Check the Status of the CAPsMAN CAP interface

CAPsMAN

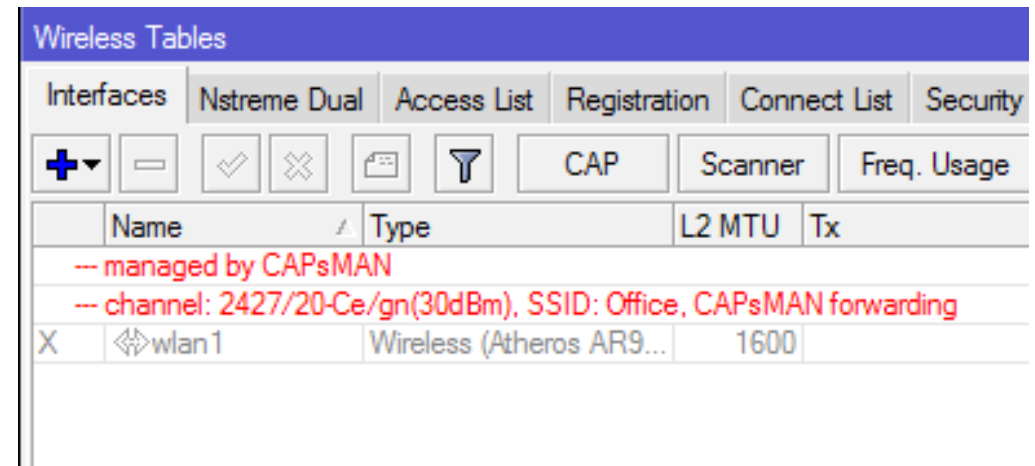


The screenshot shows the CAPsMAN configuration interface. The 'Interfaces' tab is selected, and the 'OfficeAP1' interface is highlighted. The interface is currently in a 'running-ap' state. The configuration details are as follows:

Name	Type	MTU	L2 MTU
DSMB OfficeAP1	Interfaces	1500	1600

Interface	Current State	Current Channel	Current Rate Set	Current Basic Rate Set
<OfficeAP1>	running-ap	2427/20-Ce/gn(30dBm)	CCK:1-11 OFDM:6-54 BW:1x-2x HT:0-7	OFDM:6 BW:1x HT:0-7

CAP



The screenshot shows the Wireless Tables configuration interface. The 'CAP' tab is selected, and the 'wlan1' interface is highlighted. The interface is currently in a 'down' state. The configuration details are as follows:

Name	Type	L2 MTU	Tx
X wlan1	Wireless (Atheros AR9...	1600	

Additional information displayed in red text:

- managed by CAPsMAN
- channel: 2427/20-Ce/gn(30dBm), SSID: Office, CAPsMAN forwarding

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

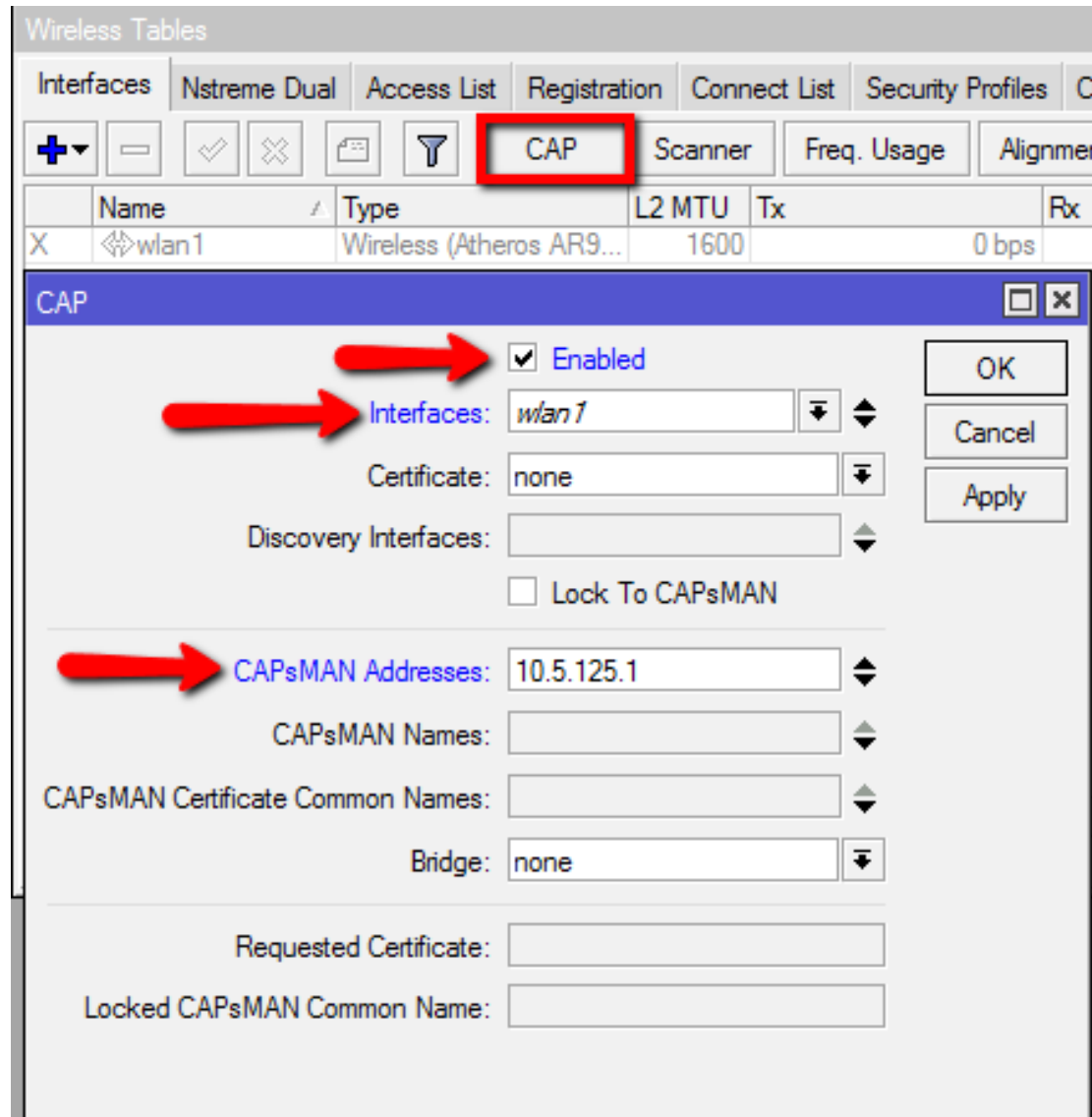
- MAC Layer2:
 - No IP configuration required
 - CAP and CAPsMAN must be in the same Layer 2 network
- IP (UDP) Layer3:
 - CAP must reach the CAPsMAN using IP protocol
 - Can traverse NAT if necessary
- Management connection between CAP and CAPsMAN is secured using DTLS
- CAP client data traffic is not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



The screenshot shows the Mikrotik WinBox interface for configuring a CAP (Client Authentication Profile). The 'CAP' tab is selected in the 'Wireless Tables' window. The configuration dialog is open, showing the following settings:

- Enabled:** (indicated by a red arrow)
- Interfaces:** wlan1 (indicated by a red arrow)
- Certificate:** none
- Discovery Interfaces:** (empty)
- Lock To CAPsMAN:**
- CAPsMAN Addresses:** 10.5.125.1 (indicated by a red arrow)
- CAPsMAN Names:** (empty)
- CAPsMAN Certificate Common Names:** (empty)
- Bridge:** none
- Requested Certificate:** (empty)
- Locked CAPsMAN Common Name:** (empty)

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

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

Enabled

Interfaces:

Certificate:

Discovery Interfaces:

Lock To CAPsMAN

CAPsMAN Addresses:

CAPsMAN Names:

CAPsMAN Certificate Common Names:

Bridge:

Requested Certificate:

Locked CAPsMAN Common Name:

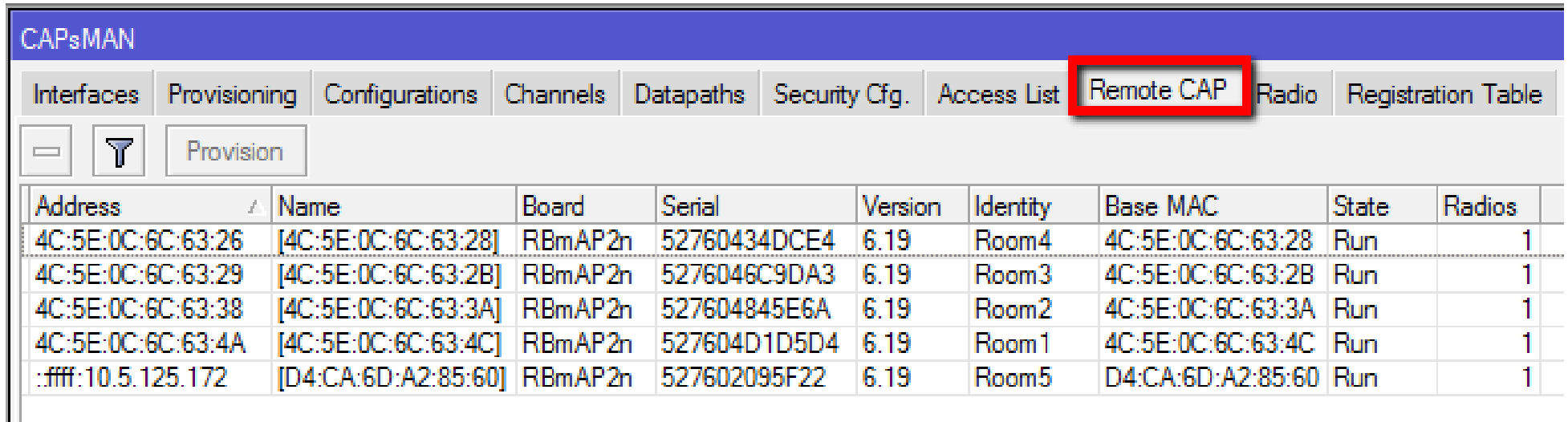
OK

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' and a filter icon. 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, 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 configuration for the selected interface 'OfficeAP5' is shown. A red box highlights the 'Copy' button. A red arrow points from this 'Copy' button to the 'New Interface' dialog box. In the 'New Interface' dialog, the name is changed to 'Room5AP', and a red box highlights the 'OK' button.

Interface <OfficeAP5>

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

Name: OfficeAP5
Type: Interfaces
MTU: 1500
L2 MTU: 1600
MAC Address: D4:CA:6D:A2:85:60
ARP: enabled
Radio MAC: D4:CA:6D:A2:85:60
Master Interface: none

Buttons: OK, **Copy**, Remove, Torch

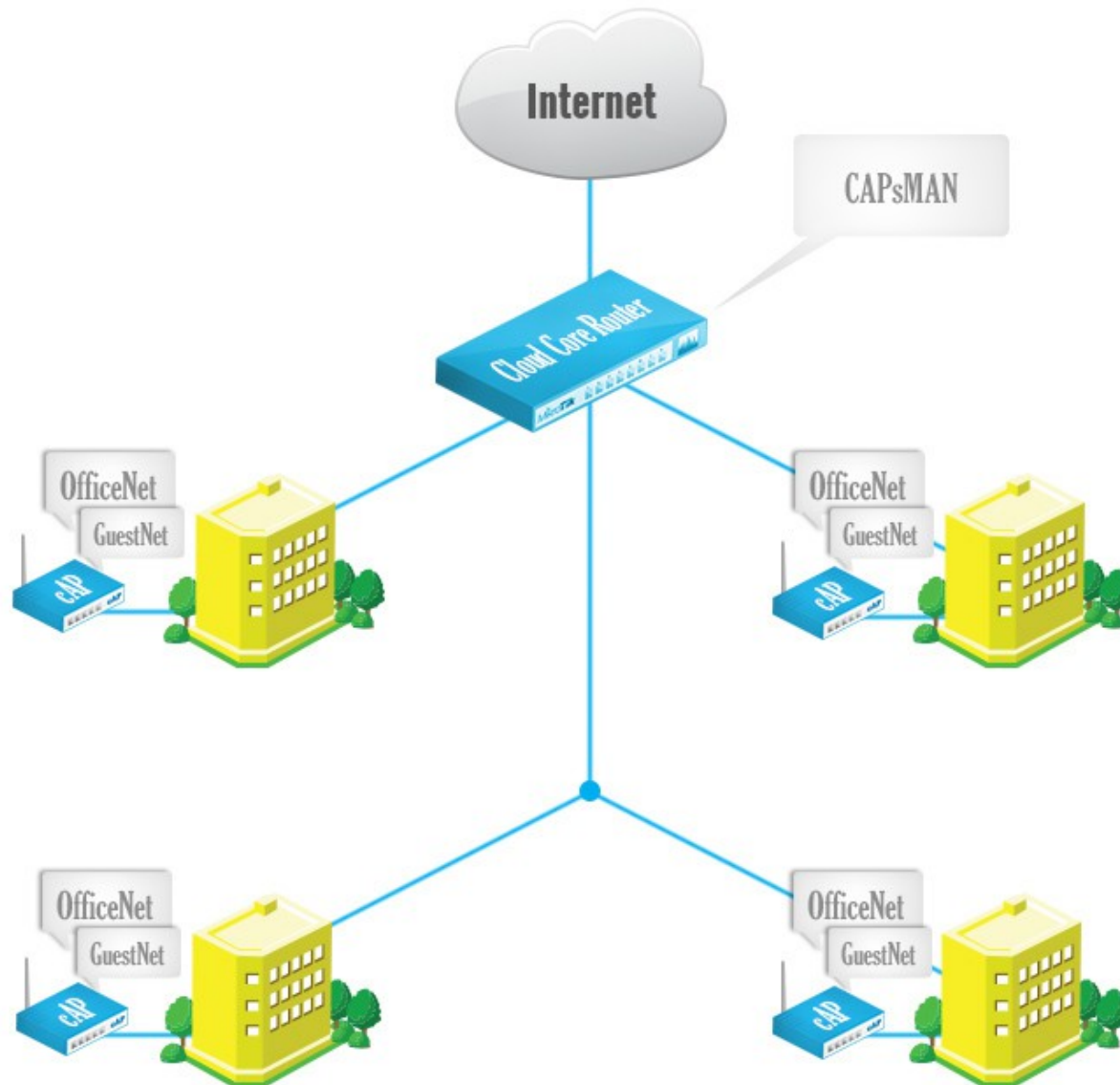
New Interface

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

Name: Room5AP
Type: Interfaces
MTU: 1500
L2 MTU: 1600
MAC Address: D4:CA:6D:A2:85:60
ARP: enabled
Radio MAC: D4:CA:6D:A2:85:60
Master Interface: none

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

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 web interface. At the top, the 'Configurations' tab is selected and highlighted with a red box. Below the tabs, a table lists existing configurations. The 'New CAPs Configuration' panel is open, showing the 'Wireless' sub-tab selected with a red box. Within this panel, the 'Datapath' sub-tab is also highlighted with a red box. The configuration form includes the following fields:

Name	SSID	Hide SSID	Load Bal...	Country	Channel	Frequency	Band	D
OfficeNet	Office			united sta...				

New CAPs Configuration			
Wireless	Channel	Datapath	Security
Name:	GuestNet	Datapath:	
Mode:		Bridge:	GuestNet
SSID:	Guest	Bridge Cost:	
Hide SSID:		Bridge Horizon:	
Load Balancing Group:		Local Forwarding:	
Country:		Client To Client Forwarding:	
Max Station Count:		VLAN Mode:	
Multicast Helper:		VLAN ID:	
HT Tx Chains:			
HT Rx Chains:			
HT Guard Interval:			

CAPsMAN VirtualAP Setup

CAPsMAN

Interfaces **Provisioning** Configurations Channels Datapaths Sec

+ - ✓ ✗ 📁 🔍

#	Radio MAC	Action	Master Configurati...	Slave C
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

+ - ✓ ✗ 📄 🔍 Manager AAA

	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. The 'Access List' tab is selected and highlighted with a red box. Below the tab, a table header is visible with columns: #, MAC Address, MAC Mask, Interface, Signal Ra..., Action, Client To Clie..., VLAN Mo..., and VLAN ID. A red box highlights the '+' icon in the toolbar. Two 'New CAPs Access Rule' dialog boxes are open. The left dialog shows a rule with MAC Address '18:34:51:00:00:00', MAC Mask 'FF:FF:FF:00:00:00', and Action 'accept'. The right dialog shows a rule with Action 'query radius'. Both dialogs have 'enabled' status at the bottom.

#	MAC Address	MAC Mask	Interface	Signal Ra...	Action	Client To Clie...	VLAN Mo...	VLAN ID
---	-------------	----------	-----------	--------------	--------	-------------------	------------	---------

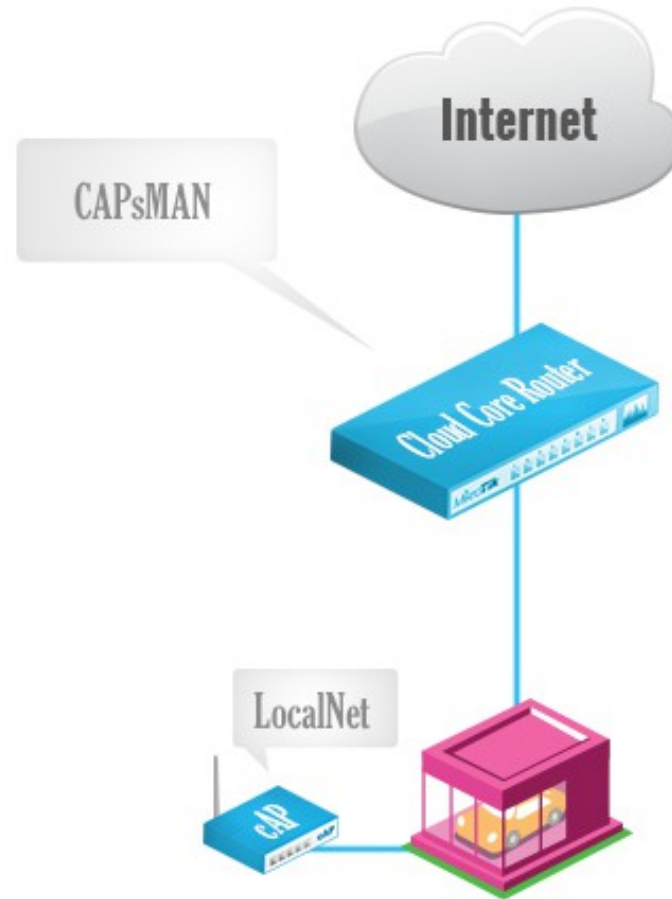
New CAPs Access Rule (Left)

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

New CAPs Access Rule (Right)

MAC Address:
MAC Mask:
Interface:
Signal Range:
Time:
Action: query radius
AP Tx Limit:
Client Tx Limit:
Private Passphrase:
Client To Client Forwarding:
RADIUS Accounting:
VLAN Mode:
VLAN ID:
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 tabs, a toolbar contains a plus sign icon, also highlighted with a red box. A table lists existing configurations:

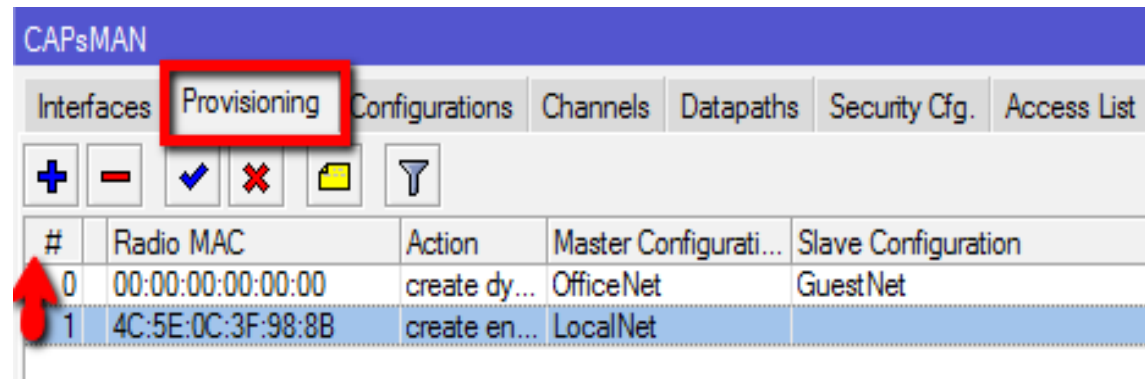
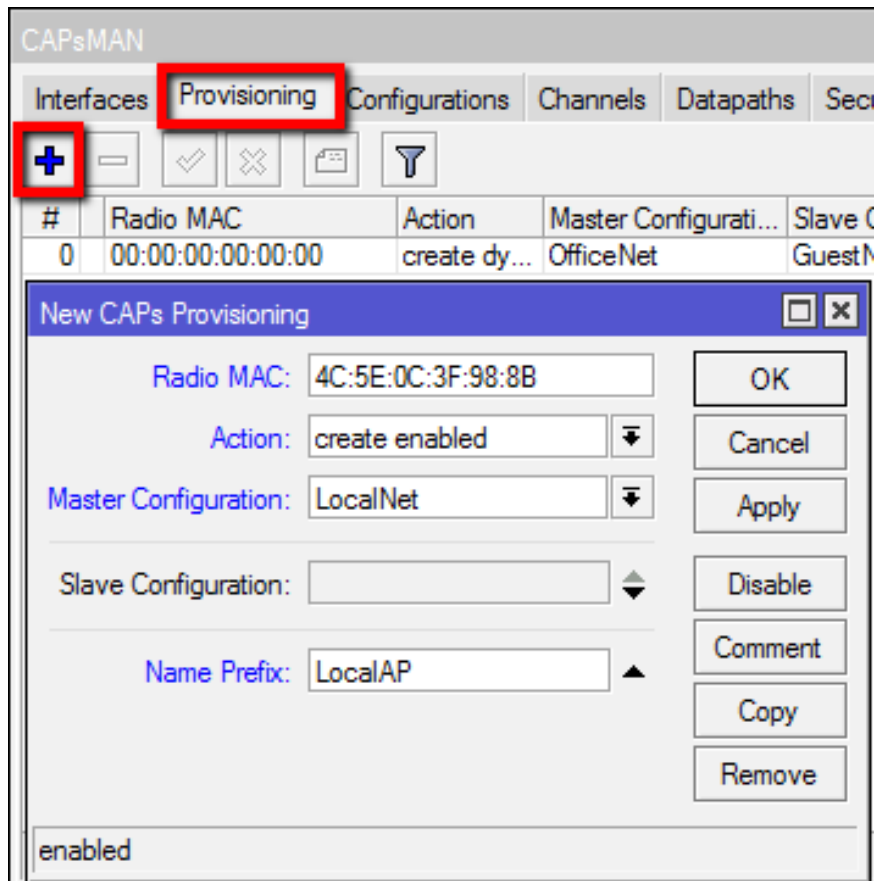
Name	SSID	Hide SSID	Load Bal...	Country	Channel	Frequency	Band	Datapath	Bridge	VLAN M...
GuestNet	Guest								GuestNet	
OfficeNet	Office			united sta...					OfficeNet	

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

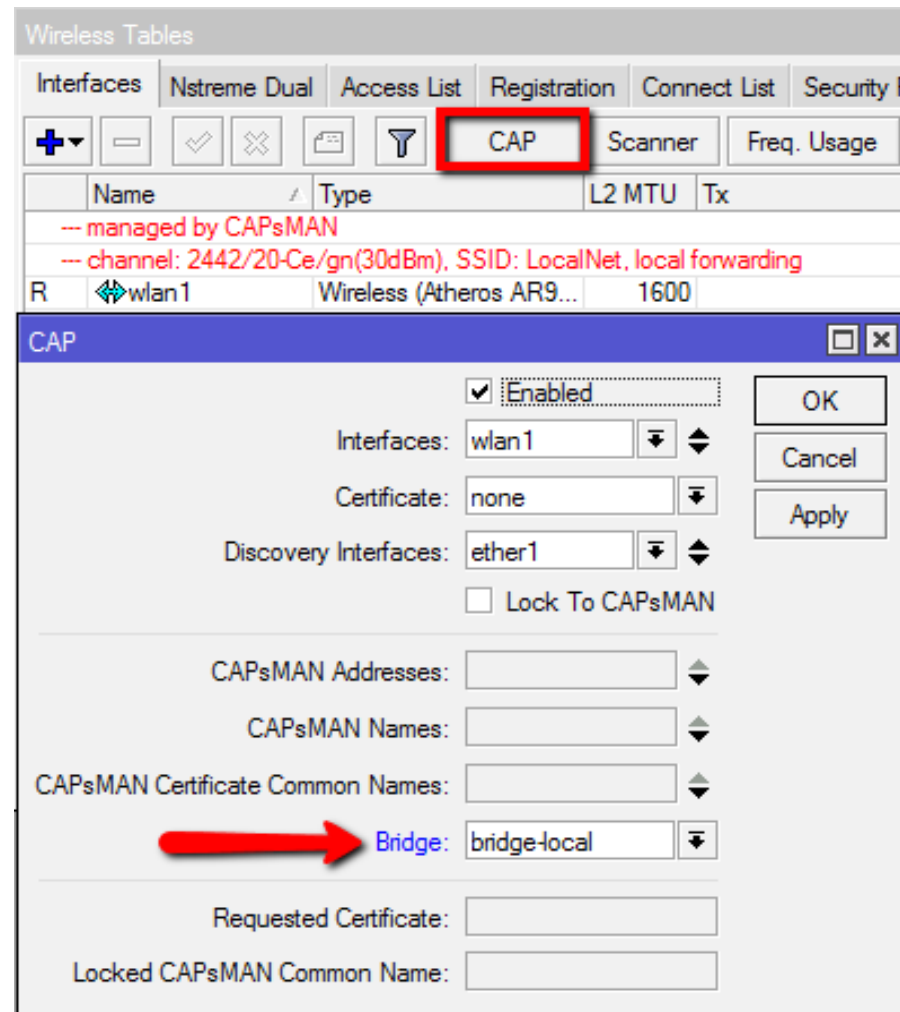
CAPsMAN Local Forwarding

- 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 configuration panels, each with a 'Channel' tab highlighted in red. The panels are:

- CAPs Configuration <Both Bands>**: Channel, Datapath, Security. Channel: [], Frequency: [], Width: 20, Band: 5ghz-a/n, Extension Channel: [], Tx. Power: []
- CAPs Configuration <5ghz Config>**: Channel, Datapath, Security. Channel: [], Frequency: [], Width: 20, Band: 5ghz-a/n, Extension Channel: [], Tx. Power: []
- CAPs Configuration <2.4ghz Config>**: Channel, Datapath, Security. Channel: [], Frequency: [], Width: [], Band: 2ghz-b/g/n, Extension Channel: [], 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

CAPsMAN

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

+ - ✓ ✗ ☰ ⏏

#	Radio MAC	Action	Master Configurati...	Slave Configuration
New CAPs Provisioning				
	Radio MAC: 00:00:00:00:00:00			
	Hw. Supported Modes: an			
	gn			
	Action: create dynamic enabled			
	Master Configuration: Both Bands			
	Slave Configuration:			
	Name Prefix:			
New CAPs Provisioning				
	Radio MAC: 00:00:00:00:00:00			
	Hw. Supported Modes: an			
	Action: create dynamic enabled			
	Master Configuration: 5ghz Config			
	Slave Configuration:			
	Name Prefix:			
New CAPs Provisioning				
	Radio MAC: 00:00:00:00:00:00			
	Hw. Supported Modes: gn			
	Action: create dynamic enabled			
	Master Configuration: 2.4ghz Config			
	Slave Configuration:			
	Name Prefix:			

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 and CAP in one board

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

Wireless Tables

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

+ - ✓ ✗ [CAP] Scanner Freq. Usa

Name	Type	L2 MTU	Tx
CAP			

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 with columns for Name, Type, MTU, L2 MTU, and Tx. The interface 'cap1' is selected. Below this, the 'Wireless Tables' section is visible, showing a table with columns for Name, Type, L2 MTU, Tx, and Rx. A red box highlights the text: '--- managed by CAPsMAN' and '--- channel: 2442/20-Ce/gn(24dBm), SSID: LocalAP, CAPsMAN forwarding'. The bottom section shows the configuration for 'Interface <cap1>' with tabs for General, Wireless, Channel, Datapath, Security, Status, and Traffic. A red box highlights the 'Current Channel' field, which is set to '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'.

Name	Type	MTU	L2 MTU	Tx
cap1	Interfaces	1500	1600	

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

Interface <cap1>

Current State: running-ap

Current Channel: 2442/20-Ce/gn(30dBm)

Current Rate Set: CCK:1-11 OFDM:6-54 BW:1x-2x HT:0-15

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.