



CAPsMAN_{v2}

Σύστημα Κεντρικής Διαχείρισης Access Point

MUM Greece – Νοέμβριος 2019



Λίγα λόγια για μένα

- Μαραγκουδάκης Σταύρος
- Ιδιοκτήτης της **HellasCOM Μ.ΕΠΕ** δημιουργός του **LinkShop.GR**
- MikroTik Certified Trainer
- Εκπαιδευτής στο **MikroTikTraining.gr**
- Πιστοποιήσεις MikroTik



- Άλλες πιστοποιήσεις



Σχετικά το MikroTikTraining.gr

- Το MikroTikTraining.gr δημιουργήθηκε με αποκλειστικό σκοπό την διοργάνωση επίσημων εκπαιδευτικών σεμιναρίων της **MikroTik**
- Προέρχεται από την εταιρία **Hellascom ΕΠΕ** (Ηλεκτρονικό κατάστημα **Linkshop.gr**) που διοργανώνει εκπαιδευτικά σεμινάρια MikroTik από το 2011 και είναι το **1ο MikroTik Training Center** στην Ελλάδα, και την εταιρία **DC ELECTRONICS**



Το ηλεκτρονικό κατάστημα LinkShop.gr προέρχεται από την εταιρία HellasCom Μ. ΕΠΕ που είναι ο 1^{ος} επίσημος MikroTik διανομέας στην Ελλάδα από το 2001!

Για τους επαγγελματίες παρέχεται η δυνατότητα **χονδρικής** στα Προϊόντα " **MikroTik & λοιπά προϊόντα** " Συμπληρώστε την **αίτηση B2B** που θα βρείτε στο **LinkShop.gr**

www.linkshop.gr

Πρόγραμμα Παρουσίασης

Ενότητα 1. **Εισαγωγή στον CAPsMAN**

Ενότητα 2. **Προαπαιτούμενα**

Ενότητα 3. **Παράμετροι CAPsMAN**

Ενότητα 4. **Παράμετροι CAP**

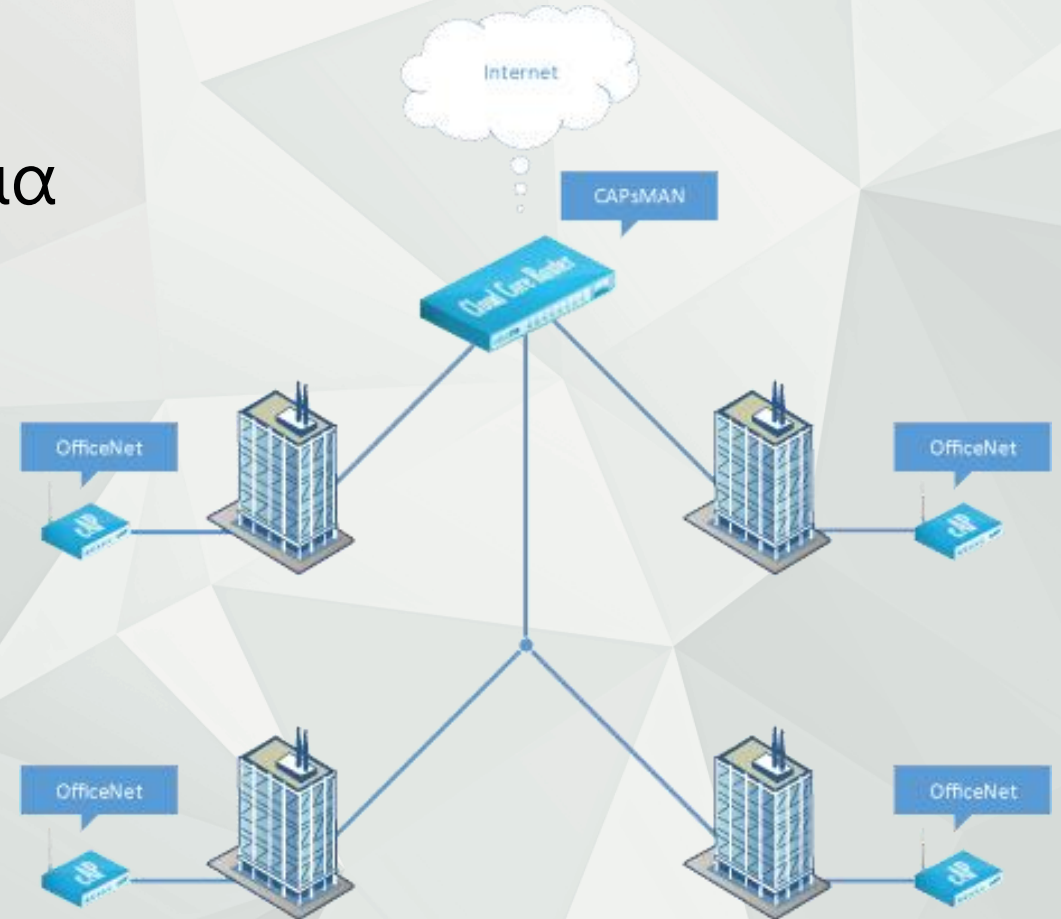
Ενότητα 5. **Έξτρα Λειτουργίες**

Ενότητα 1. Εισαγωγή στον CAPsMAN

Επισκόπηση, Χαρακτηριστικά, Εξέλιξη

CAPsMAN | Τι είναι

- Είναι μια λειτουργία του **RouterOS**
- Προσφέρει μια κεντρική πλατφόρμα διαχείρισης Wireless Access Points
- Υπάρχει σε κάθε συσκευή MikroTik
- Είναι ΔΩΡΕΑΝ



CAPsMAN | Χαρακτηριστικά

1. Κεντρική διαχείριση APs με λειτουργικό RouterOS
2. Υποστήριξη Dual Band (2,4GHz & 5GHz)
3. Provisioning των APs
4. Επικοινωνία Layer2 (MAC) και Layer3 (IP) με APs
5. Υποστήριξη Certificates στην επικοινωνία των APs
6. Δυνατότητα ισομοιρασμού πελατών
7. Λειτουργία δρομολόγησης από τοπικό δίκτυο
8. RADIUS MAC authentication
9. Υποστήριξη προσαρμοσμένης παραμετροποίησης

CAPsMAN | Ορισμοί

CAPsMAN

- Controlled Access Point system Manager
- Κεντρικός ελεγκτής Access Point

CAP

- Controlled Access Point
- RouterOS Access Point

CAPsMAN | Εξέλιξη

- Το 2014 παρουσιάστηκε ο CAPsMAN v1 και ενσωματώθηκε στο package **Wireless-fp** στην έκδοση 6.11rc1 του RouterOS
- Το 2015 κυκλοφόρησε ο CAPsMAN v2 ο οποίος ενσωματώθηκε στο νέο package **Wireless-cm2** στην έκδοση 6.23 του RouterOS
- Το 2016 στην έκδοση 6.37, καταργήθηκαν τα package **Wireless-fp** και **Wireless-cm2** και αντικαταστάθηκαν από το **Wireless-rep** το οποίο μετονομάστηκε σε **wireless**

Ενότητα 2.

Προαπαιτούμενα CAPsMAN

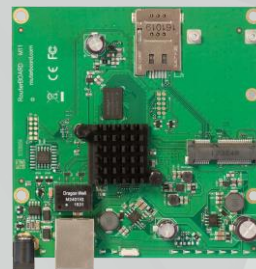
Απαιτήσεις Υλικού, Επικοινωνία

CAPsMAN | Απαιτήσεις

Απαιτείται η ύπαρξη τουλάχιστον ενός **CAPsMAN**
(Κεντρικού ελεγκτή Wireless Access Points)

- **CAPsMAN**

- Συσκευή **RouterBoard**, **x86** ή **Virtual Machine** (CHR)



VM

CAPsMAN | Απαιτήσεις

Απαιτείται η ύπαρξη τουλάχιστον ενός **CAP**
(Wireless Access Points για διαχείριση)

- **CAP**

- Συσκευή **MikroTik RouterBoard** ή **x86**
- Να διαθέτει τουλάχιστον ένα Ασύρματό Interface με chipset Atheros (a/b/g/n/ac)
- Να διαθέτει τουλάχιστον Level4 αδείας RouterOS



CAPsMAN | Επικοινωνία CAP με CAPsMAN

- **Layer2 (MAC)**

- CAP και CAPsMAN πρέπει να είναι στο δίκτυο
- Δεν απαιτείται παραμετροποίηση IP

- **Layer3 (IP)** προτεινόμενο

- CAP και CAPsMAN μπορεί να είναι σε διαφορετικό δίκτυο
- Ο CAP θα πρέπει να έχει την δυνατότητα να επικοινωνήσει με τον CAPsMAN με IP
- Λειτουργεί και πίσω από NAT

- Η επικοινωνία μεταξύ CAP και CAPsMAN είναι ασφαλής με την χρήση DTLS (Μόνο για την διαχείριση των CAPs).
- Η κίνηση των client του CAP δεν είναι κρυπτογραφημένη. Αν απαιτείται κρυπτογράφηση, χρησιμοποιείστε κάποιο Tunnel

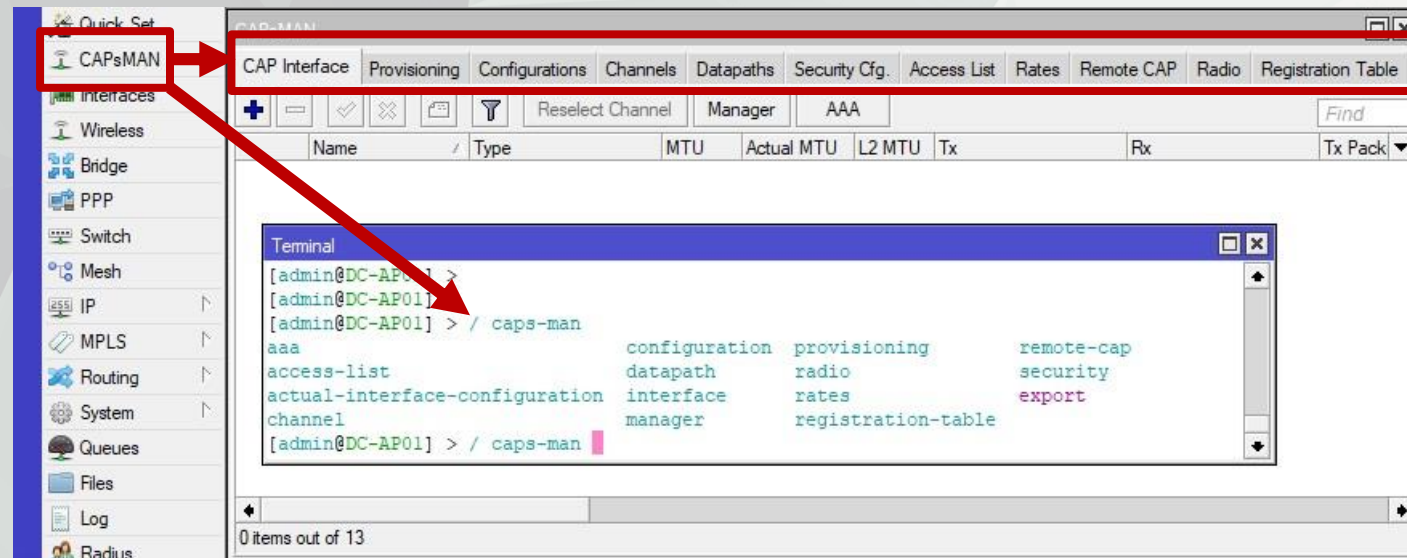
Ενότητα 3.

Παραμέτροι CAPsMAN

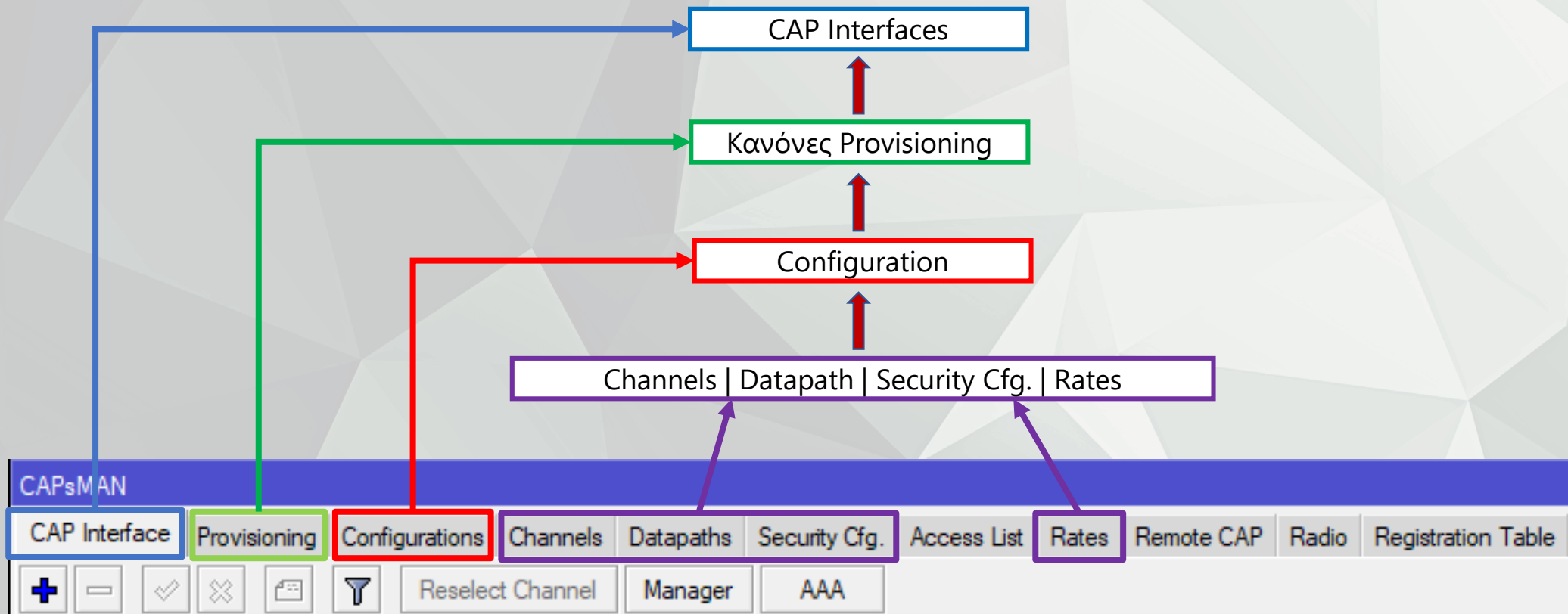
Επισκόπηση και Λειτουργίες, Επικοινωνία, Διαχείριση CAPsMAN και CAP, Ασφάλεια και Provisioning

CAPsMAN | Μενού

- Interfaces
- Provisioning
- Configuration
- Channels
- Datapaths
- Security Cfg.
- Access List
- Rates
- Remote CAP
- Radio
- Registration Table



CAPsMAN | Ιεραρχία παραμέτρων



CAPsMAN | Ιεραρχία παραμέτρων

Channels | Datapath | Security Cfg. | Rates

CAP Interface	Provisioning	Configurations	Channels	Datapaths	Security Cfg.	Access
+ - [icon] [icon]						
Name	Frequency	Control Chann...	Band	Extension Cha...	Tx Power	
2.4_Channel	2412, 2437, 2462	20Mhz	2ghz-g/n	disabled	10	

CAP Interface	Provisioning	Configurations	Channels	Datapaths	Security Cfg.	Access List	Rates
+ - [icon] [icon]							
Name	Bridge	Local For...	Client To ...	VLAN Mo...	VLAN ID		
dp1	br-private			use tag	10		

CAP Interface	Provisioning	Configurations	Channels	Datapaths	Security Cfg.	Access List	Rates	Remote CAP
+ - [icon] [icon]								
Name	Authentication Type	Encryption	Group Encryption	Group Key Update	Passphrase			
WPA2	WPA2 PSK	aes ccm	aes ccm		*****			

CAP Interface	Provisioning	Configurations	Channels	Datapaths	Security Cfg.	Access List	Rates	Remote CAP	Radio	Registration Table
+ - [icon] [icon]										
Name	Basic Rates	Supported Rates	HT Basic MCS	HT Supported MCS	VHT Basic MCS	VHT Supported MCS				
rate-profile		9Mbps 12Mbps 18Mb...		3 4 5 6 7 11 12 13 14	none	MCS 0-7, MCS 0-8, M...				

CAPsMAN | Ιεραρχία παραμέτρων

Configuration

CAPs Configuration <Master-Config>

Wireless Channel Rates Datapath Security

Name: Master-Config

Mode: ap

SSID: MikroTikTraining.gr

Hide SSID: []

Load Balancing Group: TrainingCenter

Distance: indoors km

Hw. Retries: 4

Hw. Protection Mode: []

Frame Lifetime: []

Disconnect Timeout: []

Keepalive Frames: []

Country: greece

Installation: []

Max Station Count: []

Multicast Helper: default

HT Tx Chains: 0 1 2

HT Rx Chains: 0 1 2

HT Guard Interval: []

OK Cancel Apply Comment Copy Remove

CAPs Configuration <Master-Config>

Wireless Channel Rates Datapath Security

Channel: 2.4_Channel

Frequency: []

Control Channel Width: []

Band: []

Extension Channel: []

Tx Power: []

Save Selected: []

OK Cancel Apply Comment Copy Remove

CAPs Configuration <Master-Config>

Wireless Channel Rates Datapath Security

Rate: rate-profile

Basic Rates

Supported Rates

HT Basic MCS

HT Supported MCS

VHT Basic MCS

VHT Supported MCS

OK Cancel Apply Comment Copy Remove

CAPs Configuration <Master-Config>

Wireless Channel Rates Datapath Security

Datapath: dp1

MTU: []

L2 MTU: []

ARP: []

Bridge: []

Bridge Cost: []

OK Cancel Apply Comment Copy Remove

CAPs Configuration <Master-Config>

Wireless Channel Rates Datapath Security

Security: WPA2

Authentication Type: []

Encryption: []

Group Encryption: []

Group Key Update: []

Passphrase: []

Disable PMKID: []

OK Cancel Apply Comment Copy Remove

CAPsMAN | Provisioning

Ο CAPsMAN εκτελεί τους κανόνες provisioning με τις παραμέτρους που καθορίζουμε

The image displays two side-by-side screenshots of the CAPsMAN provisioning configuration window. Both windows are titled 'CAPs Provisioning <00:00:00:00:00:00>' and show a 'Radio MAC' of '00:00:00:00:00:00'. The left window is for a 2.4G configuration, and the right window is for a 5G configuration. Red boxes highlight the following fields in both:

- Hw. Supported Modes:** 'gn' (left) and 'ac' (right)
- Identity Regexp:** 'mAP.*' (left) and 'cAP_AC.*' (right)
- IP Address Ranges:** '10.0.0.10-10.0.0.40' (left) and '10.0.0.50-10.0.0.99' (right)
- Action:** 'create disabled' (both)
- Master Configuration:** 'Master-Config_2.4G' (left) and '2ndSSID-Config_5G' (right)
- Slave Configuration:** '2ndSSID-Config_2.4G' (left) and '2ndSSID-Config_5G' (right)
- Name Format:** 'prefix identity' (both)
- Name Prefix:** '2.4G_' (left) and '5G_' (right)

Buttons on the right side of each window include OK, Cancel, Apply, Disable, Comment, Copy, and Remove. The status at the bottom of each window is 'enabled'.

CAPsMAN | **Master – Slave Configuration**

Η λειτουργία **Master – Slave** Configuration προσφέρει την δυνατότητα δημιουργίας Virtual APs (πολλαπλά SSID) σε κάθε AP

- **Master**

- Χρησιμοποιεί όλους τους Wireless παραμέτρους του Config: Frequency, channel-width, TX power

- **Slave**

- Οι Wireless παράμετροι του Config αγνοούνται
- Λαμβάνει τους παραμέτρους του Master Interface

CAPsMAN | Interfaces

Channels | Datapath | Security Cfg. | Rates

The screenshot displays the Mikrotik CAPsMAN interface configuration window. On the left, a table lists various CAP interfaces. The 'SMB' interface '2g-Room KK-103-1' is selected and highlighted. A blue box labeled 'Master Interface' points to this row. Below it, several other interfaces are listed, with a blue box labeled 'Slave Interfaces' pointing to the '2g-Room KK-104-1' interface. The main window shows the configuration for the selected interface, with tabs for General, Wireless, Channel, Rates, Datapath, Security, Status, and Traffic. The 'Channel' tab is active, showing the 'Current Channel' as '2437/20/gn(20dBm)' and the 'Current Rate Set' as 'CCK:1-11 OFDM:6-54 BW:1x SGI:1x HT:0-15'. Other fields include 'Last Link Down Time', 'Last Link Up Time', 'Link Downs', and 'Current State'. A 'Reselect Channel' button is visible at the bottom right of the configuration window.

Name	Type
SB 2g-Room KK-102-1-3	CAP Interface
SMB 2g-Room KK-103-1	CAP Interface
SB 2g-Room KK-103-1-1	CAP Interface
SB 2g-Room KK-103-1-2	CAP Interface
SB 2g-Room KK-103-1-3	CAP Interface
SMB 2g-Room KK-104-1	CAP Interface
SB 2g-Room KK-104-1-1	CAP Interface
SB 2g-Room KK-104-1-2	CAP Interface
SB 2g-Room KK-104-1-3	CAP Interface
SMB 2g-Room KK-105-1	CAP Interface
SB 2g-Room KK-105-1-1	CAP Interface
SB 2g-Room KK-105-1-2	CAP Interface
SB 2g-Room KK-105-1-3	CAP Interface
SMB 2g-Room KK-106-1	CAP Interface

452 items out of 484 (1 selected)

Interface <2g-Room KK-103-1>

General Wireless Channel Rates Datapath Security Status Traffic

Last Link Down Time: Jan/19/2019 10:48:35

Last Link Up Time: Jan/19/2019 10:48:15

Link Downs: 14

Current State: running-ap

Current Channel: 2437/20/gn(20dBm)

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

Current Basic Rate Set: CCK:1-11

Current Registered Clients: 0

Current Authorized Clients: 0

OK Cancel Apply Disable Comment Copy Remove Torch Scan... Reselect Channel

Ενότητα 4. Παραμετροι CAP

Ενεργοποίηση, Modes, HA

CAPsMAN | Ενεργοποίηση CAP

The screenshot illustrates the steps to enable a CAP in Mikrotik WinBox:

- 1**: Select the **Wireless** menu item in the left sidebar.
- 2**: Select the **CAP** option in the **Wireless Tables** list.
- 3**: In the **CAP** configuration window, check the **Enabled** checkbox.

Name	Type	Actual
wlan1	Wireless (Atheros AR9...	

1 item out of 3

CAP configuration window:

- Enabled**
- Interfaces: []
- Certificate: none
- Discovery Interfaces: []
- Lock To CAPsMAN
- CAPsMAN Addresses: []
- CAPsMAN Names: []
- CAPsMAN Certificate Common Names: []
- Bridge: none
- Static Virtual
- Requested Certificate: []
- Locked CAPsMAN Common Name: []

CAPsMAN | Επικοινωνία σε Layer 2 (MAC)

1. Καθορίζουμε Discovery Interfaces για την επικοινωνία με τον CAPsMAN
2. Επιλέγουμε Interfaces (Wireless) που θα διαχειρίζεται ο CAPsMAN
3. Επιλέγουμε CAPsMAN Names (Προαιρετικό)
4. Ενεργοποιούμε τον CAP

CAP

Enabled

Interfaces: wlan1

Certificate: none

Discovery Interfaces: ether1

Lock To CAPsMAN

CAPsMAN Addresses:

CAPsMAN Names: CAPsMAN_1

CAPsMAN Certificate Common Names:

Bridge: none

Static Virtual

Requested Certificate:

Locked CAPsMAN Common Name:

OK

Cancel

Apply

CAPsMAN | Επικοινωνία σε Layer 3 (IP)

1. Καθορίζουμε την διεύθυνση IP του CAPsMAN
2. Επιλέγουμε Interfaces (Wireless) που θα διαχειρίζεται ο CAPsMAN
3. Ενεργοποιούμε τον CAP

The screenshot shows the 'CAP' configuration window. The 'Enabled' checkbox is checked. The 'Interfaces' dropdown is set to 'wlan1'. The 'CAPsMAN Addresses' dropdown is set to '10.0.10.1'. Other fields include 'Certificate: none', 'Discovery Interfaces: ', 'Lock To CAPsMAN' (unchecked), 'CAPsMAN Names: ', 'CAPsMAN Certificate Common Names: ', 'Bridge: none', 'Static Virtual' (unchecked), 'Requested Certificate: ', and 'Locked CAPsMAN Common Name: '.

CAPsMAN | High Availability

Σε κρίσιμες εφαρμογές όπου απαιτείται High Availability, μπορούμε να εισάγουμε στα CAP περισσότερους CAPsMANs.

Σε περίπτωση που υπάρχει δυσλειτουργία στον 1^ο CAPsMAN, το CAP θα συνδεθεί στον επόμενο.

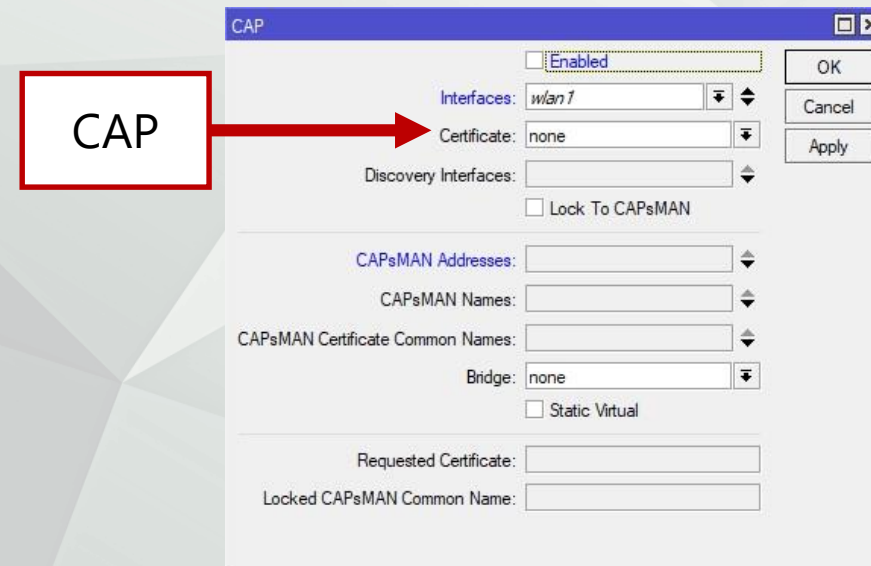
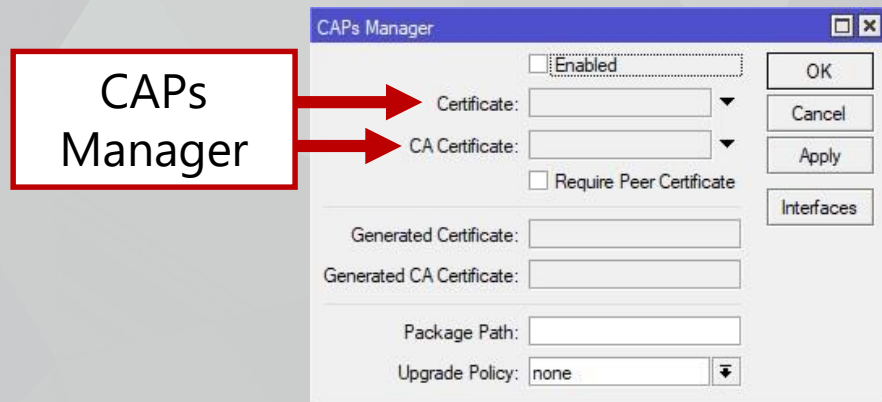
The screenshot shows the 'CAP' configuration window in Mikrotik WinBox. The 'Enabled' checkbox is checked. The 'Interfaces' field contains 'wlan1' and 'wlan2'. The 'Certificate' field is set to 'none'. The 'Discovery Interfaces' field is empty. The 'Lock To CAPsMAN' checkbox is unchecked. The 'CAPsMAN Addresses' field is highlighted with a red box and contains three entries: '10.0.0.1', '10.0.0.2', and '192.168.1.1'. The 'CAPsMAN Names' field is also highlighted with a red box and contains two entries: 'Master_CAPsMAN' and 'Slave_CAPsMAN'. The 'CAPsMAN Certificate Common Names' field is empty. The 'Bridge' field is set to 'none' and the 'Static Virtual' checkbox is unchecked. The 'Requested Certificate' and 'Locked CAPsMAN Common Name' fields are empty. The window has 'OK', 'Cancel', and 'Apply' buttons.

Ενότητα 5. Έξτρα λειτουργίες **CAPsMAN**

Auto-Certification, Access List, Load Balance, Local Forwarding

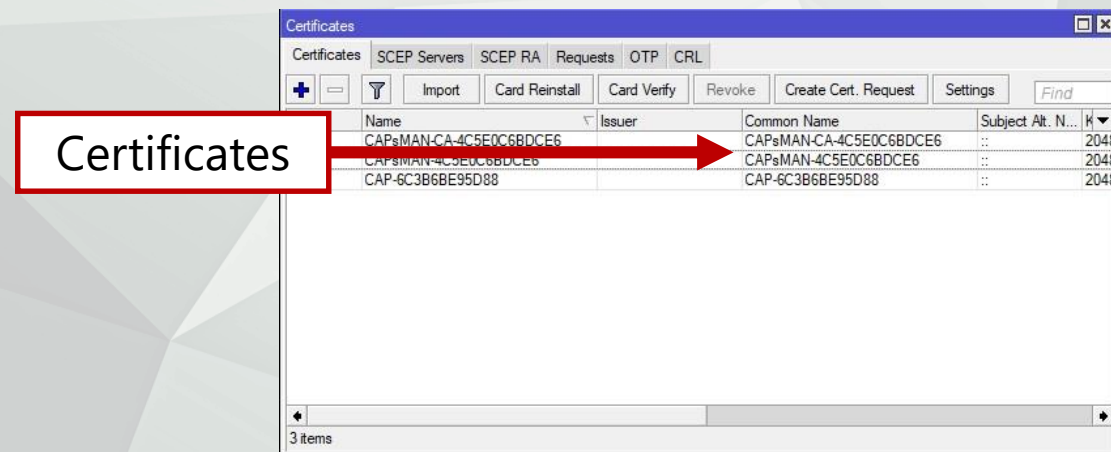
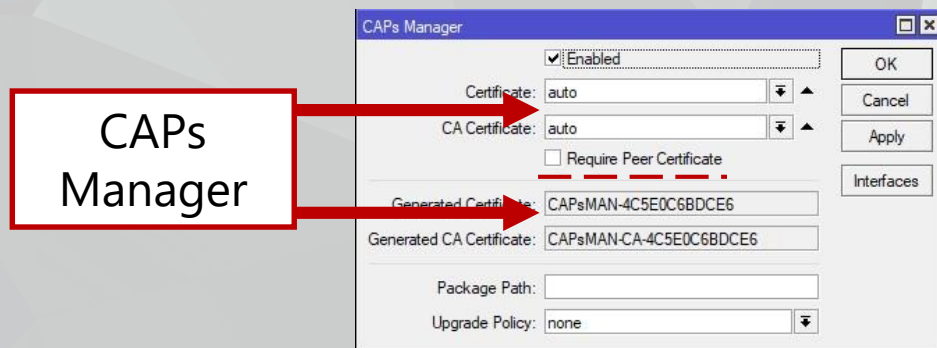
CAPsMAN | Auto Certification

- Ο τύπος Authentication επιλέγεται στον Manager:
 - Χωρίς authentication
 - Υποχρεωτική χρήση certification



CAPsMAN | Auto Certification

- Με το auto certification δημιουργούμε κλειδιά PKI
- CAPsMAN-CA- <mac address> (Self-signed CA)
- CAPsMAN- <mac address>



CAPsMAN | Access List

Η Access List προσφέρει καθορισμού κανόνων για τον έλεγχο πρόσβασής των clients στο WiFi.

New CAPs Access Rule

MAC Address: 80:5E:C0:80:5E:C0

MAC Mask: 80:5E:C0:00:00:00

Interface: [dropdown]

SSID Regexp: [text]

Signal Range: -80..120

Allow Signal Out Of Range: 00:00:10 [dropdown]

Time

Time: 08:00:00 - 15:00:00

Days: sun mon tue wed thu fri sat

Action: accept [dropdown]

AP Tx Limit: [text]

Client Tx Limit: [text]

Private Passphrase: CustomKey

Client To Client Forwarding:

RADIUS Accounting: [text]

VLAN Mode: use tag [dropdown]

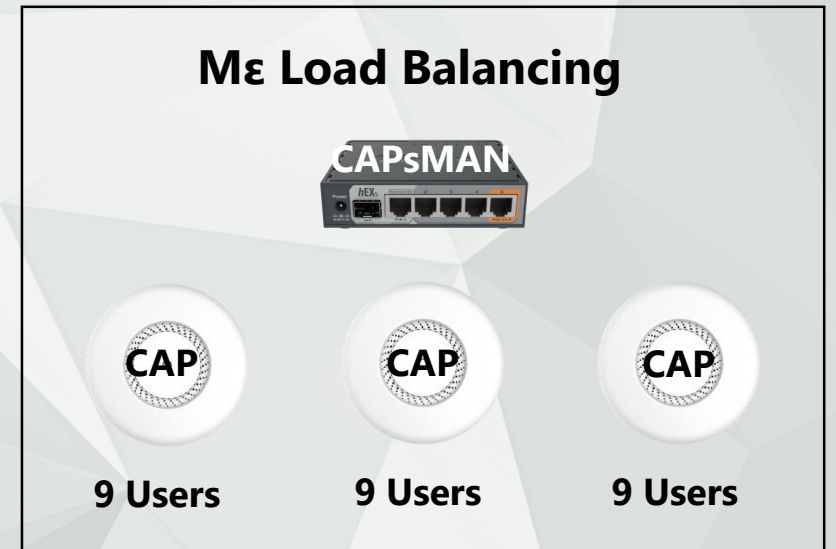
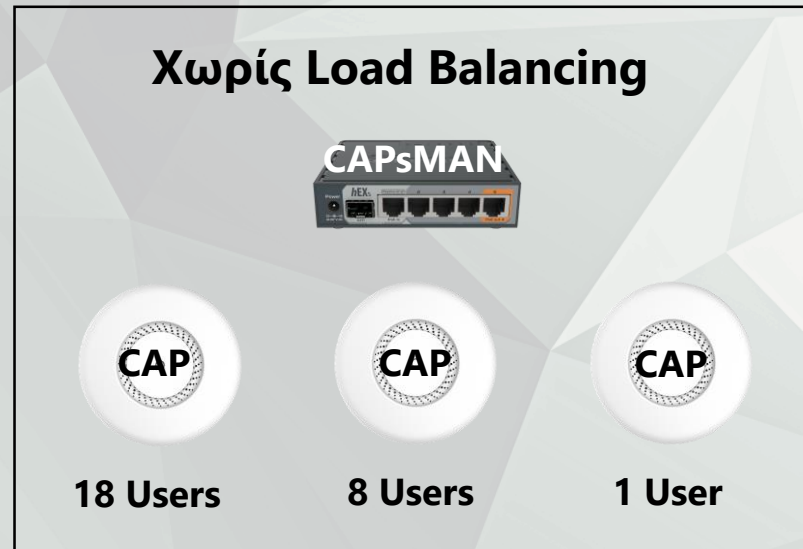
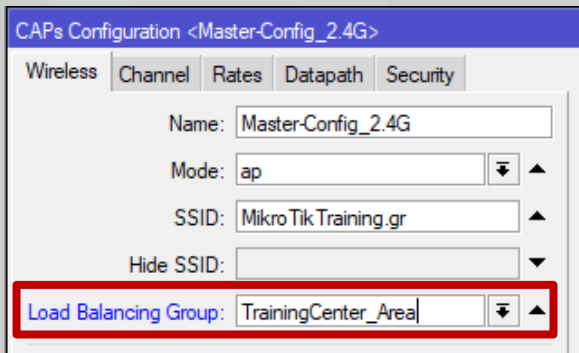
VLAN ID: 11

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

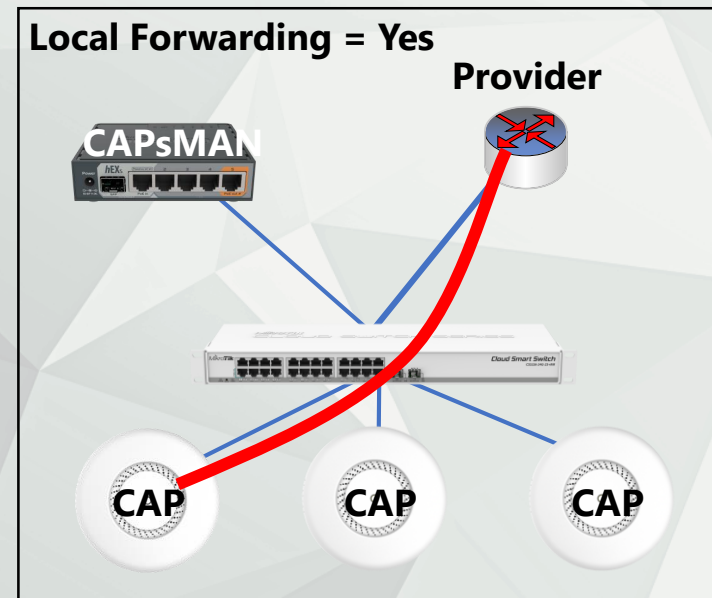
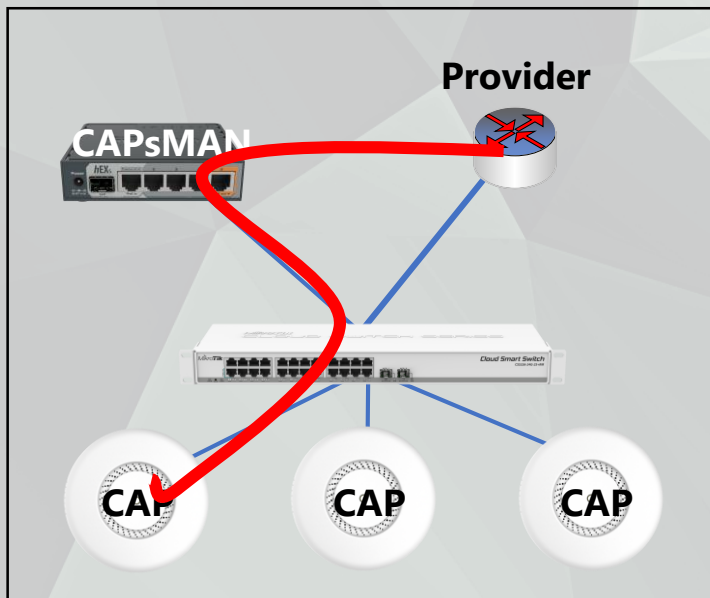
CAPsMAN | Load Balance

Η λειτουργία Load Balancing Group προσφέρει την δυνατότητα ομαδοποίησης των Access Point που βρίσκονται τον ίδιο χώρο, ώστε ο CAPsMAN να φροντίζει τον ισομοιρασμό των clients μεταξύ τους.



CAPsMAN | Datapath 'local forwarding'

Ενεργοποιώντας την λειτουργία 'Local forward' στις ρυθμίσεις του Datapath, η κίνηση των πελατών παύει να δρομολογείται μέσω του CAPsMAN και δρομολογείται από το τοπικό Bridge του Access Point





CAPsMANv2

Controlled Access Point system Manager

Σας ευχαριστώ για την προσοχή σας

