



CAPsMAN

Recent changes, spectrum usage, security features



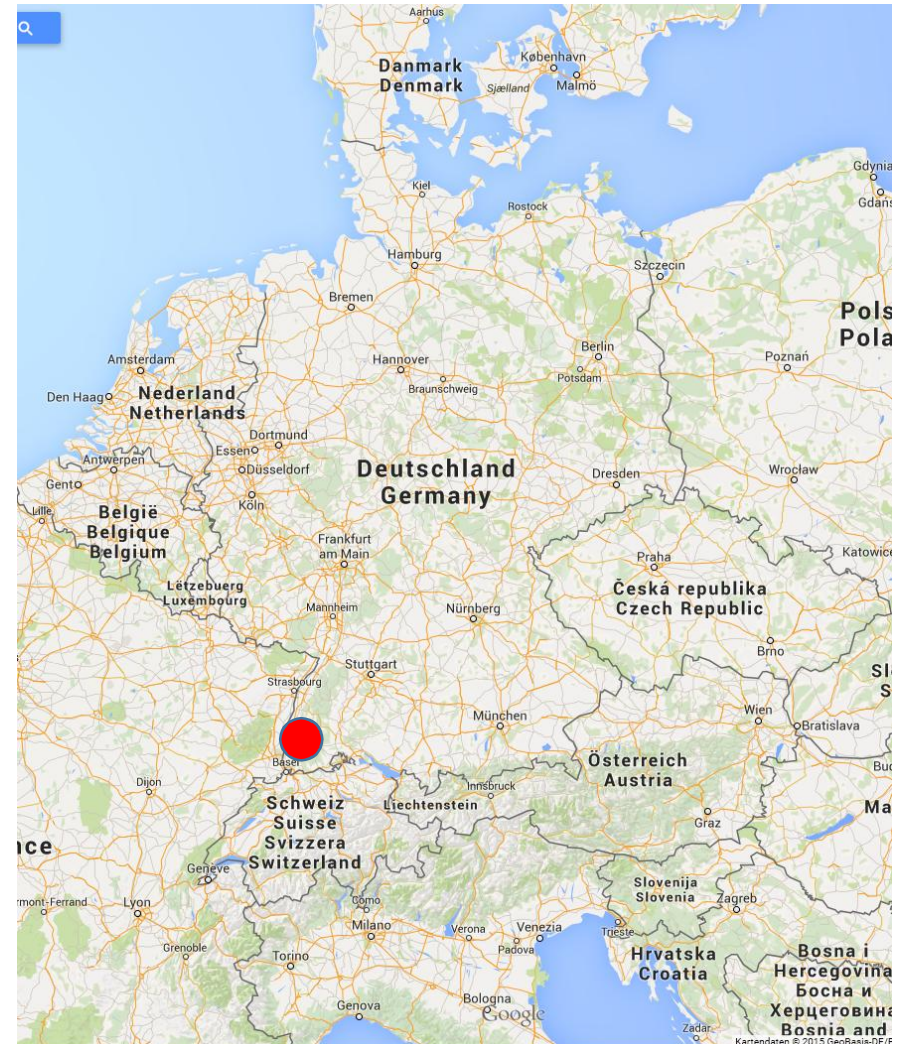
FMS Internetservice GmbH

Company Profile



FMS Internetservice GmbH

- Value Added Distributor
 - Distribution
 - Training
 - Consulting
 - Support
- Founded 1997
- 11 employees
- Southern Germany





Get in Touch

- Website: <http://www.fmsweb.de>
- MikroTik Mirror: <http://www.mikrotik-software.de>
- Shop: <http://www.mikrotik-shop.de>
- Wiki: <http://wiki.fmsweb.de>
- Twitter: https://twitter.com/fmsweb_de
- Facebook: <https://www.facebook.com/fmsinternetservice>

- Phone: +49 761 2926500
- Email: sales@fmsweb.de



Training Center

- Official MikroTik trainings
- All certification levels
- First German speaking partner
- Two trainers
- Own training facility
- Inquiries: sales@fmsweb.de

Sebastian Inacker: TR11

Patrik Schaub: TR23





Distributor Table



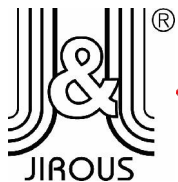
Alcatel·Lucent



SUB10
systems.com

MARS ANTENNAS & RF SYSTEMS LTD.

MikroTik



Stella Doradus
Excellence in design





Distributor Table

Live Demonstrations:

- Nokia Vplus setup
- Nokia AMS demonstration
- CRS 10G on 10 meter copper
(see tomorrow's CRS presentation)



Distributor Table



Do you need towers or masts? Contact sales@fmsweb.de



CAPsMAN

What is it about and how to get it running



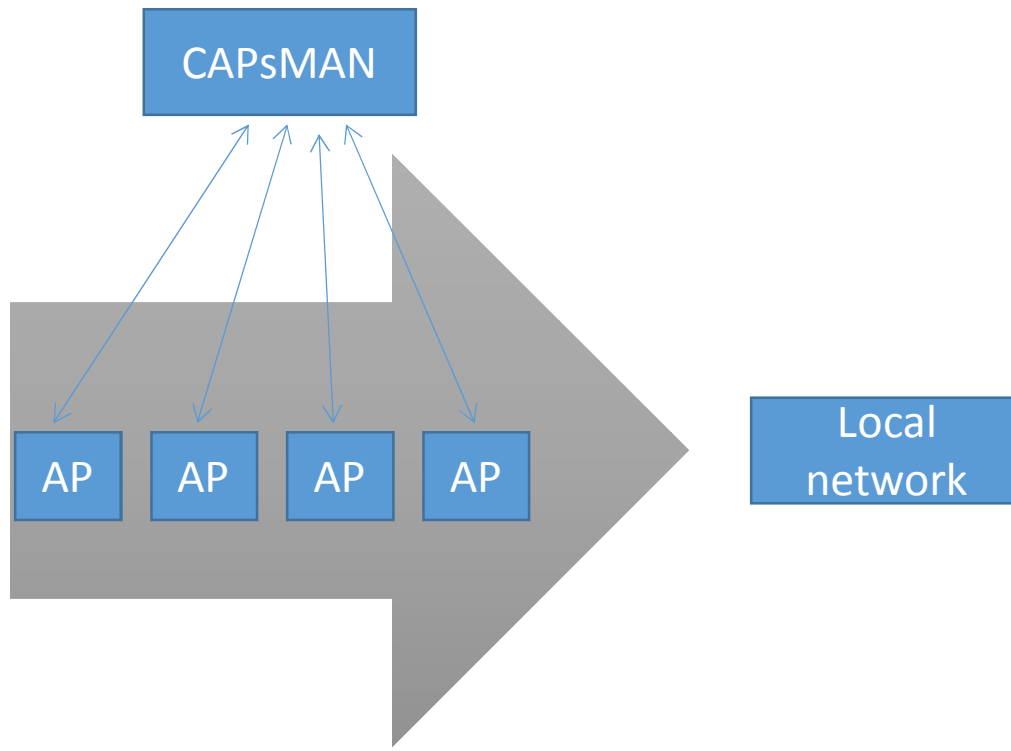
CAPsMAN Basic Features

- Provisioning (configuration) of access points
- Authentication and access control of clients
- Handling of client traffic
- Monitoring of client connections



Client Traffic: Local Forwarding

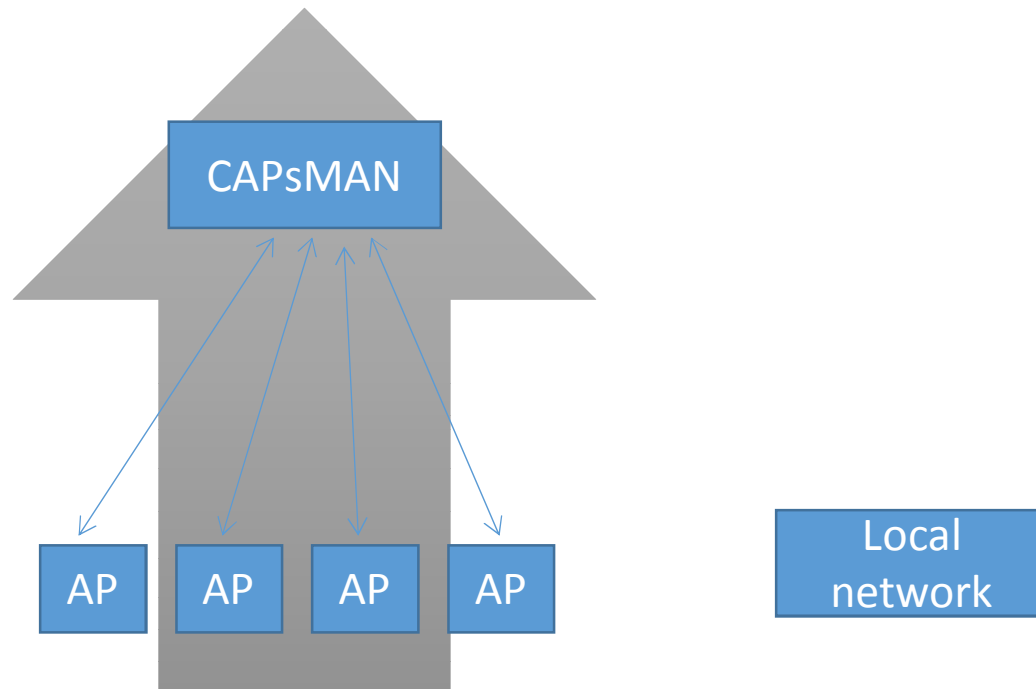
- Access point handles traffic
- Manual access point configuration





Manager Forwarding

- CAPsMAN handles traffic
- No access point configuration
- Automatic UDP tunnel



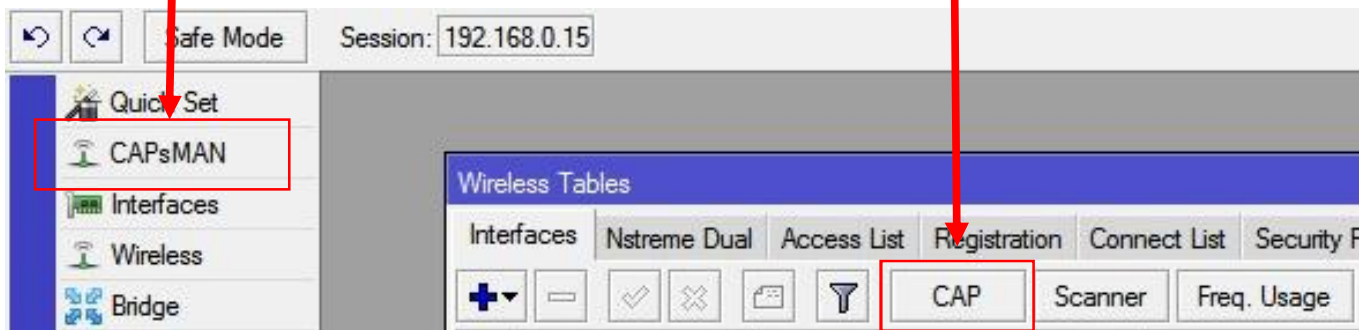


Getting Started

- Install CAPsMAN package (on old ROS versions)
- Configure CAPsMAN
- Create provisioning and config on CAPsMAN
- Configure APs (CAPs) to use manager

CAPsMAN configuration

CAP configuration





Minimum CAP Configuration (Layer 2)

- Enable
- Choose CAP interfaces
- Choose discovery interfaces

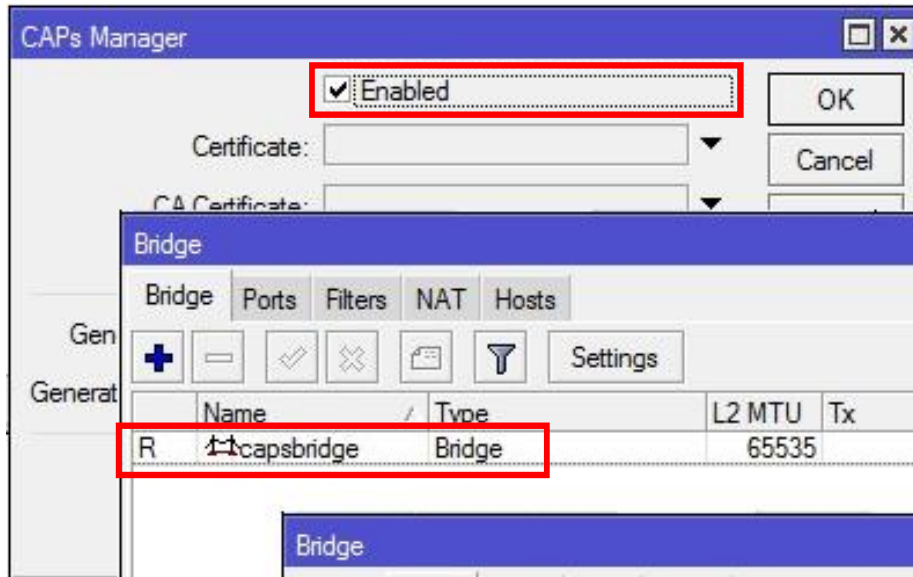
The image shows a screenshot of a configuration window titled "CAP". The window has a blue title bar with standard window controls (minimize, maximize, close). The main content area is light gray. A red rectangular box highlights the following fields:

- A dropdown menu with a checkmark and the text "Enabled".
- A text field labeled "Interfaces:" containing the value "wlan 1".
- A text field labeled "Certificate:" containing the value "none".
- A text field labeled "Discovery Interfaces:" containing the value "ether1".

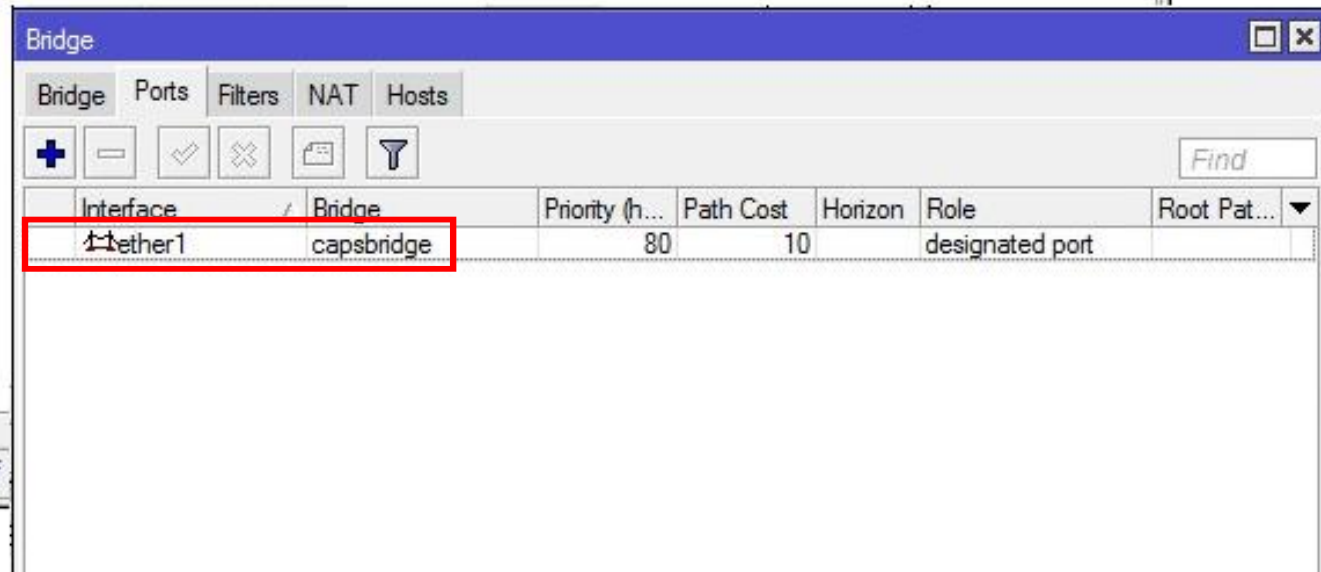
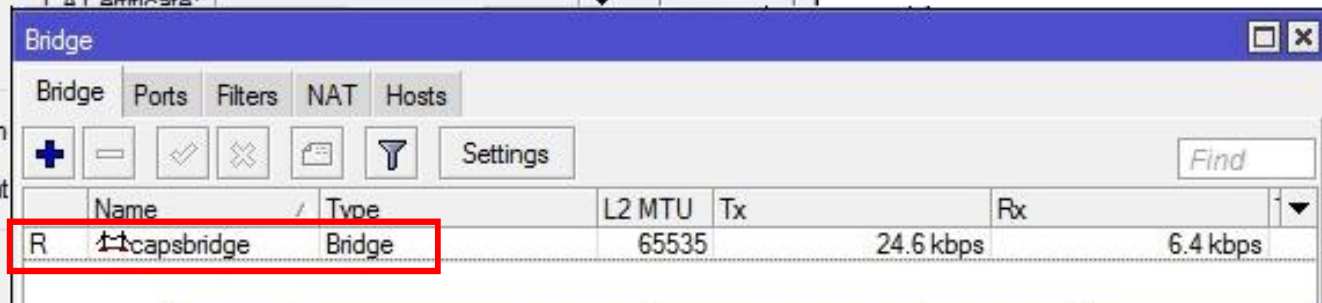
Below the highlighted area, there is a checkbox labeled "Lock To CAPsMAN" which is currently unchecked. At the bottom of the window, there are two more text fields: "CAPsMAN Addresses:" and "CAPsMAN Names:", both of which are empty. On the right side of the window, there are three buttons: "OK", "Cancel", and "Apply".



Minimum CAPsMAN Configuration



- Enable



- Create bridge
- Add port



Minimum CAPsMAN Configuration

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

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

Hw. Supported Modes: [dropdown]

Identity Regexp: [text]

Common Name Regexp: [text]

IP Address Ranges: [dropdown]

Action: create dynamic enabled

Master Configuration: cfg-6.36rc16

Slave Configuration: [dropdown]

Name Format: cap

Name Prefix: [dropdown]

enabled

CAPs Configuration <cfg-6.36rc16>

Wireless Channel Rates Datapath Security

Name: cfg-6.36rc16

Mode: [dropdown]

SSID: capstest

Hide SSID: [dropdown]

CAPs Configuration <cfg-6.36rc16>

Wireless Channel Rates Datapath Security

Datapath: [dropdown]

Bridge: capsbridge

Bridge Cost: [dropdown]

Bridge Horizon: [dropdown]

Local Forwarding: [dropdown]

Client To Client Forwarding: [dropdown]

VLAN Mode: [dropdown]

VLAN ID: [dropdown]

- Provisioning (Condition/Action)
- Wireless Config: SSID
- Datapath Config: Bridge



Latest CAPsMAN Features

See what's new



Changes wireless-rep Package

wireless-cm2

The screenshot shows the 'New CAPs Configuration' dialog box for the 'wireless-cm2' package. The 'Wireless' tab is selected. The 'Band' dropdown is set to '2ghz-b'. The 'Extension Channel' list is open, showing options: '2ghz-b', '2ghz-b/g', '2ghz-b/g/n', '2ghz-onlyg', '2ghz-onlyn', '5ghz-a', '5ghz-a/n', '5ghz-a/n/ac', '5ghz-onlyac', and '5ghz-onlyn'. The 'Tx. Power' field is empty.

wireless (formerly wireless-rep)

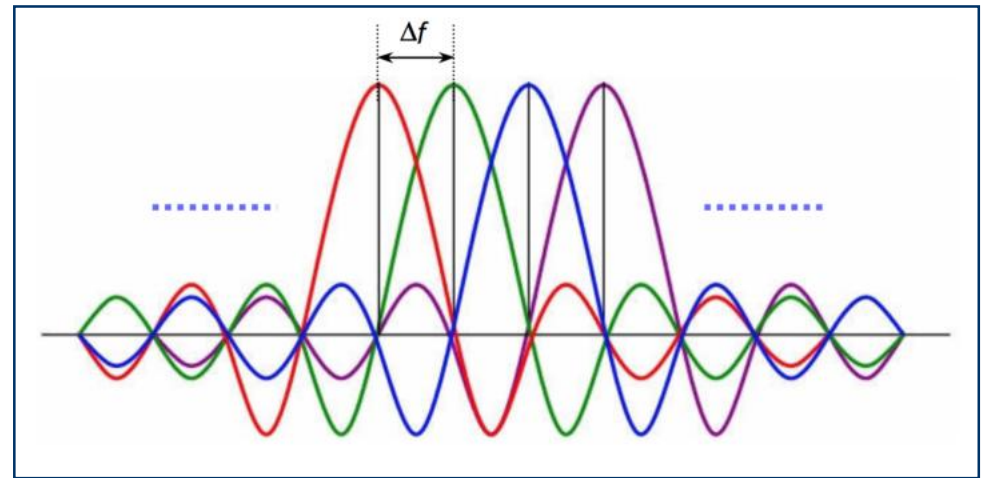
The screenshot shows the 'New CAPs Configuration' dialog box for the 'wireless (formerly wireless-rep)' package. The 'Wireless' tab is selected. The 'Band' dropdown is set to '2ghz-b'. The 'Extension Channel' list is open, showing options: '2ghz-b', '2ghz-b/g', '2ghz-b/g/n', '2ghz-g/n', '2ghz-onlyg', '2ghz-onlyn', '5ghz-a', '5ghz-a/n', '5ghz-a/n/ac', '5ghz-onlyac', and '5ghz-onlyn'. The 'Tx. Power' field is set to '2ghz-g/n', which is highlighted with a red box. On the right side of the dialog, there are buttons for 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and 'Remove'.

- Optimize 2.4GHz performance
- Disable 802.11b legacy mode



Optimize performance w/o 802.11b

- 802.11b uses DSSS modulation
- 802.11g/n uses OFDM modulation
- OFDM nodes have to take care on DSSS nodes
- DSSS nodes use more air time





Latest Changes: Discovery Interface

- List of interfaces, CAPsMAN will listen for CAPs
- For bridges: use bridge, not port

Current Stable

CAPs Manager

Enabled

Certificate:

CA Certificate:

Require Peer Certificate

Generated Certificate:

Generated CA Certificate:

Package Path:

Upgrade Policy:

OK

Cancel

Apply

Current RC

CAPs Manager

Enabled

Certificate:

CA Certificate:

Require Peer Certificate

Generated Certificate:

Generated CA Certificate:

Package Path:

Upgrade Policy:

OK

Cancel

Apply

Interfaces

CAPs Manager Interfaces

Interface	Forbid	
CAPsBridge	no	
all	yes	

2 items



Latest Changes: Static Virtual

- capsman - added support for static virtual interfaces on CAP;

The screenshot shows the Mikrotik WinBox interface for configuring a CAP (Client Access Point) profile. The 'CAP' tab is selected in the top menu. A dialog box titled 'CAP' is open, showing the following configuration options:

- Enabled
- Interfaces: wlan1
- Certificate: none
- Discovery Interfaces: ether1
- Lock To CAPsMAN
- CAPsMAN Addresses: [empty]
- CAPsMAN Names: [empty]
- CAPsMAN Certificate Common Names: [empty]
- Bridge: none
- Static Virtual

The 'Static Virtual' checkbox is highlighted with a red box, and a red arrow points from the 'CAP' tab in the top menu to this checkbox. The background shows a table with columns for Name, Type, Actual MTU, Tx, Rx, Tx Packet (p/s), and Rx Packet (p/s).



Latest Changes: Static Virtual

- Virtual interface e.g. individual: SSIDs, security setting, traffic forwarding (VLAN, bridging ...)
- New virtual interface with each CAPsMAN connect

Wireless Tables

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

Wireless Tables

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

CAP | WPS Client | Setup Repeater | Scanner

Name	Type	Actual MTU	Tx	Rx
-- managed by CAPsMAN				
-- channel: 2422/20-Ce/gn(30dBm), SSID: guest, CAPsMAN forwarding				
X wlan1	Wireless (Atheros AR9...	1500		0 bps
X wlan7	Virtual			0 bps
-- managed by CAPsMAN				
-- SSID: staff_local forwarding				
DR wlan8	Virtual	1500		0 bps



Latest Changes: Static Virtual

- Local forwarding: enabled interface
- Local interface configuration necessary
- E.g. local traffic handling:
 - Forwarding traffic to VLAN
 - By using virtual interface as bridge port



Latest Changes: Static Virtual

Interface List

Interface	Interface List	Ethernet	PWR	EoIP Tunnel	IP Tunnel	GR
R	ether1	Ethernet				
RS	vlan1	VLAN				
	ether2	Ethernet				
	ether3	Ethernet				
	ether4	Ethernet				
	ether5	Ethernet				
R	staff-bridge	Bridge				
-- managed by CAPsMAN						
-- channel: 2422/20-Ce/gn(30dBm), SSID: guest, CAPsMAN forwarding						
X	wlan1	Wireless (Atheros AR9...				
-- managed by CAPsMAN						
-- SSID: staff_local forwarding						
DRS	wlan2	Virtual				

9 items (1 selected)

Bridge

Interface	Bridge	Priority (h...	Path Cost	Horizon
staff-vlan1	staff-bridge	80	10	
staff-wlan2	staff-bridge	80	10	

Interface List

Interface	Interface List	Ethernet	PWR	EoIP Tunnel	IP Tunnel	GR
R	ether1	Ethernet				
RS	vlan1	VLAN				
	ether2	Ethernet				
	ether3	Ethernet				
	ether4	Ethernet				
	ether5	Ethernet				
R	staff-bridge	Bridge				
-- managed by CAPsMAN						
-- channel: 2422/20-Ce/gn(30dBm), SSID: guest, CAPsMAN forwarding						
X	wlan1	Wireless (Atheros AR9...				
-- managed by CAPsMAN						
-- SSID: staff_local forwarding						
DR	wlan3	Virtual				

9 items (1 selected)

Bridge

Interface	Bridge	Priority (h...	Path Cost	Horizon
unknown	staff-bridge	80	10	
staff-vlan1	staff-bridge	80	10	



Latest Changes: Static Virtual

- wlan7 just disabled, not removed

Wireless Tables

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

+ | - | ✓ | ✗ | 📄 | 🗑️ | CAP | WPS Client | Setup Repeater | Scanner | Freq. Usage | Alignm

	Name	Type	Actual MTU	Tx	Rx	Tx Pack
-- managed by CAPsMAN						
X	wlan1	Wireless (Atheros AR9...	1500	0 bps	0 bps	
X	wlan7	Virtual		0 bps	0 bps	

2 items out of 9

CAP

Enabled

Interfaces: wlan1

Certificate: none

Discovery Interfaces: ether1

Lock To CAPsMAN

CAPsMAN Addresses:

CAPsMAN Names:

CAPsMAN Certificate Common Names:

Bridge: none

Static Virtual

OK

Cancel

Apply



Static Virtual vs. CAP Bridge Setting

- Dynamic bridge port
- Alternative to static virtual for
- Only one bridge
- No other settings (e.g IP, routing ...)

The screenshot displays the Mikrotik WinBox interface. At the top, the 'Wireless Tables' window is open, showing a table of wireless interfaces. The 'wlan6' interface is highlighted with a red box, showing its type as 'Virtual'. Below this, the 'CAP' configuration window for 'wlan6' is shown. The 'Enabled' checkbox is checked, and the 'Bridge' dropdown is set to 'staff-bridge'. A red box highlights the 'Bridge' dropdown and the 'Static Virtual' checkbox, which is unchecked. To the right, the 'Bridge' table is visible, showing two entries: 'ether1' connected to 'staff-bridge' and 'wlan6' connected to 'staff-bridge'. Red arrows point from the 'wlan6' entry in the 'Wireless Tables' and the 'wlan6' entry in the 'Bridge' table to the 'wlan6' CAP configuration window.

Name	Type	Actual MTU	Tx
-- managed by CAPsMAN			
-- channel: 2427/20-Ce/gn(30dBm), SSID: guest2, CAPsMAN forwarding			
X wlan1	Wireless (Atheros AR9...	1500	0 bps
-- managed by CAPsMAN			
-- SSID: staff_local forwarding			
DRS wlan6	Virtual		

Interface	Bridge
ether1	staff-bridge
D wlan6	staff-bridge

Bridge: staff-bridge
 Static Virtual



Latest Changes: Save Selected

- Save selected channel
- No frequency set = “auto”
- Speeds up frequency selection on CAPsMAN start

The screenshot shows a dialog box titled "CAPs Channel <channel1>". It contains several input fields and a list of buttons. The "Name" field is filled with "channel1". The "Frequency", "Width", "Band", "Extension Channel", and "Tx Power" fields are empty. The "Save Selected" checkbox is checked and highlighted with a red border. The buttons on the right are "OK", "Cancel", "Apply", "Comment", "Copy", and "Remove".

Name:	<input type="text" value="channel1"/>	<input type="button" value="OK"/>
Frequency:	<input type="text"/>	<input type="button" value="Cancel"/>
Width:	<input type="text"/>	<input type="button" value="Apply"/>
Band:	<input type="text"/>	<input type="button" value="Comment"/>
Extension Channel:	<input type="text"/>	<input type="button" value="Copy"/>
Tx Power:	<input type="text"/>	<input type="button" value="Remove"/>
Save Selected:	<input checked="" type="checkbox"/>	



Save Selected: CAPsMAN Disabled

The screenshot displays three overlapping configuration windows for CAPsMAN interfaces. Each window has a title bar and a tabbed interface with 'Wireless', 'Channel', 'Rates', 'Datapath', 'Security', 'Status', and 'Traffic' tabs. The 'Status' tab is active in all windows.

- Interface <cap56> (leftmost window):**
 - Current State: running-ap
 - Current Channel: 2422/20-Ce
 - Current Rate Set: CCK:1-11 OFDM:6-54 BW:1x-2x SGI:1x-2x HT:0-15
 - Current Basic Rate Set: CCK:1-11
- Interface <cap57> (middle window):**
 - Current State: running-ap
 - Current Channel: 2427/20-Ce
 - Current Rate Set: CCK:1-11 OFDM:6-54 BW:1x-2x SGI:1x-2x HT:0-15
 - Current Basic Rate Set: CCK:1-11
- Interface <cap58> (rightmost window):**
 - Current State: running-ap
 - Current Channel: 2412/20-Ce/gn(30dBm)
 - Current Rate Set: CCK:1-11 OFDM:6-54 BW:1x-2x SGI:1x-2x HT:0-15
 - Current Basic Rate Set: CCK:1-11

At the bottom of each window, there is a status bar with buttons: enabled, running, slave, master, bound, and inactive. The 'inactive' button is highlighted with a red box in each window.



Save Selected: CAPsMAN Reconnect

The image displays three screenshots of the CAPsMAN configuration interface, illustrating the state of different CAPsMAN interfaces during a reconnect process. Each window shows the 'Wireless' tab with various configuration parameters.

- Interface <cap56> (State 3: Inactive):** The 'Current State' is 'running-ap' and the 'Current Channel' is '2442/20-Ce'. A red box highlights the 'Current State' field. A callout box labeled '3' with 'Inactive' points to the 'inactive' radio button at the bottom.
- Interface <cap58> (State 2: Channel selection):** The 'Current State' is 'selecting-channel' and the 'Current Channel' is '2422/20-Ce/gn(30dBm)'. A red box highlights the 'Current State' field. A callout box labeled '2' with 'Channel selection' points to the 'inactive' radio button at the bottom.
- Interface <cap57> (State 1: Running):** The 'Current State' is 'running-ap' and the 'Current Channel' is '2422/20-Ce/gn(30dBm)'. A red box highlights the 'Current State' field. A callout box labeled '1' with 'Running' points to the 'inactive' radio button at the bottom.

At the bottom of each window, there is a row of radio buttons: 'enabled', 'running', 'slave', 'master', 'bound', and 'inactive'. The 'inactive' radio button is highlighted with a red box in each screenshot.



Latest Changes: Save Selected

- Auto channel selection sequentially
- The more CAPs the longer
- Save selected saves last used channel
- Speeds up CAPsMAN restart
- Especially with many CAPs



Channel Planning and Regulation

Missing CAPsMAN Feature



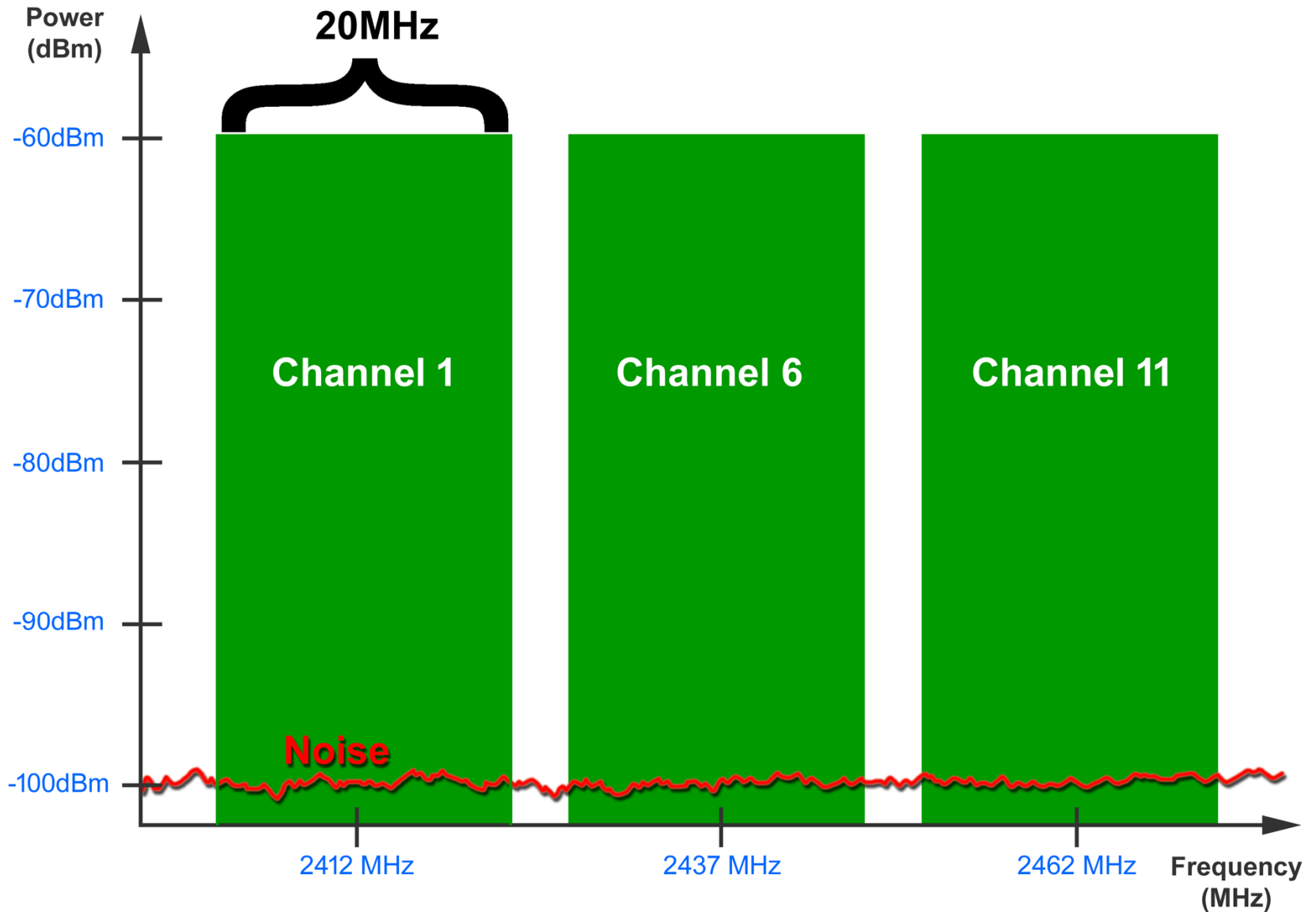
2,4GHz Channel Planning

- No channel 12/13 with FCC devices
- Public WiFi limited to channel 1 – 11
- Non overlapping channels: 1,6,11

Channel	ETSI	FCC
1	20dBm	30dBm
2	20dBm	30dBm
3	20dBm	30dBm
4	20dBm	30dBm
5	20dBm	30dBm
6	20dBm	30dBm
7	20dBm	30dBm
8	20dBm	30dBm
9	20dBm	30dBm
10	20dBm	30dBm
11	20dBm	30dBm
12	20dBm	n/a
13	20dBm	n/a



2,4GHz Channel Planning





2,4GHz Channel Planning

- Without CAPsMAN: Use Scan List & Channels

Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme Status Traffic

Mode: ap bridge

Band: 2GHz-G/N

Channel Width: 20MHz

Frequency: auto

SSID: fmsweb.de

Scan List: CH 1/6/11

Wireless Protocol: 802.11

Security Profile: wpa2

WPS Mode: disabled

Bridge Mode: enabled

VLAN Mode: no tag

VLAN ID: 1

Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles Channels

#	List	Name	Frequency (MHz)	Width (MHz)	Band	Extension Channel
0	CH 1/6/11	Channel 1	2412.000	20.000	2GHz-G/N	disabled
1	CH 1/6/11	Channel 6	2437.000	20.000	2GHz-G/N	disabled
2	CH 1/6/11	Channel 11	2462.000	20.000	2GHz-G/N	disabled



2,4GHz Channel Planning

- Problem: No scan list option in CAPsMAN
 - Configure CAPsMAN interfaces one by one?
 - Controller advantage reduced
-
- Work around using CAPsMAN strengths
 - Provisioning rules
 - Modular hierarchical configuration
 - RegEx and Overrides



Channel 1-6-11 Setup

CAPsMAN

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

+ - [Icons] Find

#	Radio MAC	Hw. Supported Modes	Identity Regexp	Action	Master Configuration
0	00:00:00:00:00:00	g	-2.4CH01	create dynamic enabled	2.4GHz CH1
1	00:00:00:00:00:00	g	-2.4CH11	create dynamic enabled	2.4GHz CH11
2	00:00:00:00:00:00	g	-2.4CH06	create dynamic enabled	2.4GHz CH6
3	00:00:00:00:00:00		none		Missing

CAPsMAN

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

+ - [Icons] Find

Name	SSID	Country	Channel	Frequency	Rate	Datapath	Sec
2.4GHz CH1	FMS	germany	2.4GHz Standard	2412MHz	StandardRates	ToCAPsBridge	WPA2
2.4GHz CH11	FMS	germany	2.4GHz Standard	2462MHz	StandardRates	ToCAPsBridge	WPA2
2.4GHz CH6	FMS	germany	2.4GHz Standard	2437MHz	StandardRates	ToCAPsBridge	WPA2
Missing							

CAPsMAN

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

+ - [Icons] Find

Name	Frequency	Width	Band	Extension Channel	Tx Power
2.4GHz Standard			20MHz 2ghz-g/n	disabled	



Channel 1-6-11 Setup

1

Require 802.11g, no Legacy support

2

Check CAP identity by RegEx for wanted channel

3

Use configuration according to RegEx

#	Radio MAC	Hw. Supported Modes	Identity Regexp	Action	Master Configuration
0	00:00:00:00:00:00	g	-2.4CH01	create dynamic enabled	2.4GHz CH1
1	00:00:00:00:00:00	g	-2.4CH11	create dynamic enabled	2.4GHz CH11
2	00:00:00:00:00:00	g	-2.4CH06	create dynamic enabled	2.4GHz CH6
3	00:00:00:00:00:00		none		Missing

4

Catch-All Rule | Avoids static interface creation

Find unwanted and misconfigured CAP (802.11b or identity not set)



Channel 1-6-11 Setup

Common central setting blocks for maximum modularity

The screenshot shows two windows from the CAPsMAN interface. The top window displays a table of channel configurations. The bottom window shows a detailed view of a channel configuration.

Name	SSID	Country	Channel	Frequency	Rate	Datapath	Sec
2.4GHz CH1	FMS	germany	2.4GHz Standard	2412MHz	StandardRates	ToCAPsBridge	WPA2
2.4GHz CH11	FMS	germany	2.4GHz Standard	2462MHz	StandardRates	ToCAPsBridge	WPA2
2.4GHz CH6	FMS	germany	2.4GHz Standard	2437MHz	StandardRates	ToCAPsBridge	WPA2
Missing							

Name	Frequency	Width	Band	Extension Channel	Tx Power
2.4GHz Standard	2412MHz	20MHz	2ghz-g/n	disabled	

Just frequency override within every configuration



Channel 1-6-11 Setup

CAPsMAN

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

+ - [Icons] Manager AAA

	Name	Type	Radio MAC	Configuration	SSID	Frequency
DSMB	cap15	CAP Interface	D4:CA:6D:4C:21:7D	2.4GHz CH6	FMS	2437MHz
DSMB	cap16	CAP Interface	6C:3B:6B:78:83:27	2.4GHz CH11	FMS	2462MHz
DSMB	cap17	CAP Interface	4C:5E:0C:C2:E4:F7	2.4GHz CH1	FMS	2412MHz

CAPsMAN

Provisioning Configurations Channels Datapaths Security Cfg. Access List Ra

[Filter Icon] Provision

	Radio MAC	Remote CAP Name	Remote CAP Identity
	6C:3B:6B:78:83:26	[6C:3B:6B:78:83:21]	CAP-Room12-2.4CH11
P	D4:CA:6D:4C:21:7D	[D4:CA:6D:4C:21:78]	CAP-Lobby-2.4CH06
P	6C:3B:6B:78:83:27	[6C:3B:6B:78:83:21]	CAP-Room12-2.4CH11
P	4C:5E:0C:C2:E4:F7	[4C:5E:0C:C2:E4:F3]	CAP-Lobby-2.4CH01

4 items

Interface uses channel 1 (2412MHz)

Identity contains „--2.4CH01“



Channel 1-6-11 Setup

CAPsMAN				
Provisioning				
Configurations				
Channels				
Datapaths				
Security Cfg.				
Access List				
Rates				
Remote CAP				
Radio				
	Provision			
	Radio MAC	Remote CAP Name	Remote CAP Identity	Interface
<input type="checkbox"/>	6C:3B:6B:78:83:26	[6C:3B:6B:78:83:21]	CAP-Room 12-2.4CH11	
P	D4:CA:6D:4C:21:7D	[D4:CA:6D:4C:21:78]	CAP-Lobby-2.4CH06	cap15
P	6C:3B:6B:78:83:27	[6C:3B:6B:78:83:21]	CAP-Room 12-2.4CH11	cap16
P	4C:5E:0C:C2:E4:F7	[4C:5E:0C:C2:E4:F3]	CAP-Lobby-2.4CH01	cap17

4 items

Interface not provisioned
Catch all rule | Action = none
Reason: not supporting 802.11g



5GHz Regulation

- Radar detection / DFS
 - Not yet possible with CAPsMAN
 - Is currently being implemented
-
- Frequencies < 5470 MHz only indoor
 - Outdoor setups without scan list?



5GHz Outdoor Channels

- Solution: etsi 5.5 – 5.7 outdoor

Country:	etsi 5.5-5.7 outdoor
Max Station Count:	croatia cyprus czech republic
Multicast Helper:	debug denmark dominican republic
HT Tx Chains:	ecuador egypt
HT Rx Chains:	egypt 5.8 el salvador
HT Guard Interval:	estonia etsi 2.4 5.5-5.7 etsi 2.4 rb411uahrb411ar etsi 5.5-5.7 outdoor etsi 5.7-5.8 srd finland france france res french guiana french polynesia

Interface <wlan2>

General Wireless Data Rates Advanced HT WDS Nstreme ..

Mode: ap bridge

Band: 5GHz-A

Channel Width: 20MHz

Frequency: auto

SSID: 5500

Radio Name: 5505
5510
5515

Scan List: 5520
5525
5530
5535

Wireless Protocol: 5540

Security Profile: 5545

WPS Mode: 5550
5555

Frequency Mode: 5560
5565
5570

Country: 5575

Antenna Gain: 5580
5585
5590
5595

WMM Support: disabled



Forcing 30dBm EIRP

- Use etsi 5.5 – 5.7 even indoors?
- Force high EIRP
- Regulation in Germany: 30dBm instead of 23dBm
- Actually 27dBm due to ATPC missing

The screenshot shows the Mikrotik WinBox configuration interface. At the top, the 'Country' is set to 'etsi 5.5-5.7 outdoor'. Below it, the 'Antenna Gain' is set to '0' dB, which is highlighted with a red box. A red arrow points from this box to the 'channel: 5500/20-Ceee/ac(27dBm)' entry in the 'Wireless Tables' section. The 'Wireless Tables' section has tabs for 'Interfaces', 'Nstreme Dual', 'Access List', 'Registration', 'Connect List', 'Security Profiles', and 'Channels'. Below the tabs are buttons for '+', '-', checkmark, cross, folder, funnel, CAP, WPS Client, Setup Repeater, Scanner, and Freq. Usage. The table below has columns for Name, Type, Actual MTU, Tx, and Rx. The table contains two entries, both marked as 'managed by CAPsMAN'. The second entry is highlighted in blue and has its channel configuration highlighted with a red box.

Name	Type	Actual MTU	Tx	Rx
---	---	---	---	---
wlan1	Wireless (Atheros AR9...	1500	0 bps	0 bps
---	---	---	---	---
wlan2	Wireless (Atheros AR9...	1500	0 bps	0 bps

Antenna gain setting of CAP accounted!



Tx Power: The more the better?

- WiFi connection is bidirectional
- Mobile devices have small Tx power

High EIRP + low gain AP antenna = pointless

- Mobile device will hear AP but can not reach it
- Unnecessary interference
- Hard to select best AP for client
- Smartphone shows full bars but can't connect
- iPhone 5 ~ 12dBm Tx, -0,8dBi = 11,2dBm EIRP



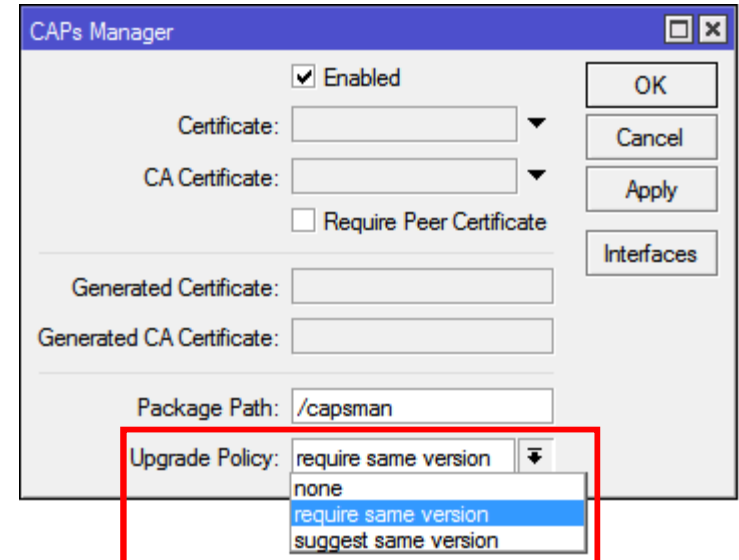
CAPsMAN Security

Keeping CAPsMAN safe



Upgrade Policy

- automatic CAP RouterOS update
- none: do nothing
- suggest: try update but accept different version
- require: try update and reject if not possible
- CAP doesn't need internet connection





Upgrade Policy

- CAP gets software packet from CAPsMAN
- Same architecture: works automatically
- Different architecture: CAP needs extra .npk

```
user admin logged in from 00:50:B6:12:FD:05 via winbox
```

```
[4C:5E:0C:C2:E4:F3/4/c921,Join,[4C:5E:0C:C2:E4:F3]] joined, provides radio(s): 4C:5E:0C:C2:E4:F7
```

```
[4C:5E:0C:C2:E4:F3/4/c921,Run,[4C:5E:0C:C2:E4:F3]] should auto upgrade
```

```
[4C:5E:0C:C2:E4:F3/4/c921,Run,[4C:5E:0C:C2:E4:F3]] ask to upgrade, version 6.39rc51
```

```
[4C:5E:0C:C2:E4:F3/4/c921,Run,[4C:5E:0C:C2:E4:F3]] upgrade status: failed, failed to download file 'routeros-smips-6.39rc51.npk', no such file
```

```
[4C:5E:0C:C2:E4:F3/4/c921,Run,[4C:5E:0C:C2:E4:F3]] upgrade failed, do not provision as same version required
```

- hAP lite (smips) CAP can't use npk of RB750UP
CAPsMAN (mipsbe)



Upgrade Policy

1

```
[4C:5E:0C:C2:E4:F3/4/3598,Run,[4C:5E:0C:C2:E4:F3]] upgrade status: failed, failed to download file 'routeros-smips-6.39rc51.npk', no such file  
[4C:5E:0C:C2:E4:F3/4/3598,Run,[4C:5E:0C:C2:E4:F3]] upgrade failed, do not provision as same version required
```

4

```
[4C:5E:0C:C2:E4:F3/4/3598,Run,[4C:5E:0C:C2:E4:F3]] removed by user request  
[4C:5E:0C:C2:E4:F3/4/91da,Join,[4C:5E:0C:C2:E4:F3]] joined, provides radio(s): 4C:5E:0C:C2:E4:F7  
[4C:5E:0C:C2:E4:F3/4/91da,Run,[4C:5E:0C:C2:E4:F3]] previously failed upgrade to version 6.39rc51, now version 6.38.5  
[4C:5E:0C:C2:E4:F3/4/91da,Run,[4C:5E:0C:C2:E4:F3]] should auto upgrade, retry  
[4C:5E:0C:C2:E4:F3/4/91da,Run,[4C:5E:0C:C2:E4:F3]] ask to upgrade, version 6.39rc51  
4C:5E:0C:C2:E4:F3/4/3598 failed to connect, timeout  
[4C:5E:0C:C2:E4:F3/4/91da,Run,[4C:5E:0C:C2:E4:F3]] upgrade status: rebooting, disconnect  
ether3 link down  
ether3 link up (speed 100M, full duplex)  
4C:5E:0C:C2:E4:F3/4/91da failed to connect, timeout  
ether3 link down  
ether3 link up (speed 100M, full duplex)  
[4C:5E:0C:C2:E4:F3/4/7be9,Join,[4C:5E:0C:C2:E4:F3]] joined, provides radio(s): 4C:5E:0C:C2:E4:F7  
[4C:5E:0C:C2:E4:F3/4/7be9,Run,[4C:5E:0C:C2:E4:F3]] previously tried auto upgrade to version 6.39rc51, now version 6.39rc51
```

2

Create folder by FTP

3

File Name	Type	Size	Creation Time
capsman	directory		Mar/12/2017 21:08:50
capsman/routeros-mipsbe-6.37.npk	package	9.4 MiB	Mar/12/2017 22:05:29
capsman/routeros-mipsbe-6.38.npk	package	9.5 MiB	Mar/12/2017 22:15:41
capsman/routeros-smips-6.39rc51.npk	package	7.2 MiB	Mar/13/2017 21:26:46
skins	directory		Jan/01/1970 01:00:53

CAPs Manager

Enabled

Certificate:

CA Certificate:

Require Peer Certificate

Generated Certificate:

Generated CA Certificate:

Package Path:

Upgrade Policy: require same version

OK Cancel Apply Interfaces



WIFI Security

Security types supported by CAPsMAN



Security Overview

- Common WPA2 PSK
- Conditional WPA2 PSK
(Access List)
- MAC based WPA2 PSK

- WPA2 EAP using local
certificates (EAP-TLS)
- WPA2 EAP using Radius (passthrough)

- Hotspot





CAPsMAN with Hotspot

- UDP tunnels directly to hotspot

1 Bridge: CAPsBridge

2 Local Forwarding:

3

Name	Interface
hotspot 1	CAPsBridge

4

Interface	Bridge
DI cap4	CAPsBridge
DI cap5	CAPsBridge
D cap6	CAPsBridge

Secure | Efficient | Scales well | Easy traffic handling



HSNM a MikroTik Hotspot Extension

Tight MikroTik integration

- Installation + update scripts
- PPPoE support
- Experienced support team



Excellent addon

- High level Captive Portal features
- Emphasis on graphical design



HS Network Manager



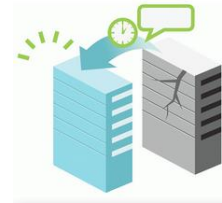
Responsive login



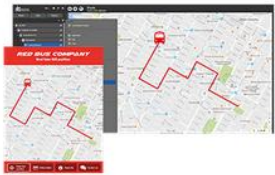
Social login



Payment options



Redundancy,
load balancing



GPS tracking
(e.g coaches)



SMS authentication



Ticket printer



Advertising, surveys,
quizzes



HS Network Manager

🇬🇧 ⓘ ⚙️ 🔌

Dashboard
System dashboard

Admin | **Data** | Search

- System
- Coffee House Ltd
- Coffee House Ltd
- CoffeeHouse
- CoffeeHouseHotspot
- HeadOffice
- World Travel Agency
- Venice Campaign

Number of connections

Chart

Users count by domain

Chart

Connections	Traffic	New users	Clicks	Impressions	CTR	Gw sold	Adv sold	HDD	RAM	CPU	NET
<small>Last 30 days</small>	<small>Last 30 days</small>	<small>Last 30 days</small>	<small>Last 30 days</small>	<small>Last 30 days</small>	<small>Last 30 days</small>	<small>Last 30 days</small>	<small>Last 30 days</small>	<small>Free space</small>	<small>Used</small>	<small>Load</small>	<small>Bandwidth (bit)</small>
30	5 Gb	3	7	33	21.21%	20.00 \$	160.00 \$	17 Gb	1 Gb	1	5 Kb 7 Kb
66.67%	100%+	0%	100%+	100%+	---	53.85%	100%+				

Top domains connections

Last 30 days

CoffeeHouse	18
HeadOffice	12

Top users traffic

Last 30 days

0014445556667@HeadOffice	1 Gb
0012223334444@HeadOffice	1 Gb
002333444455@CoffeeHouse	1 Gb
00112345678@CoffeeHouse	935 Mb
00187654321@CoffeeHouse	466 Mb
00133344455566@HeadOffice	224 Mb

Social users

Last 30 days

2

Details

- Facebook 0
- Twitter 2
- Google 0
- Standard 1

Context data

Details

Number of registered retailers	1
Number of registered managers	2
Number of registered gateways	2
Total number of connections	53
Number of registered users	11
Number of activated users	6
Total sold by retailers and by invoice	58.00
Sales of other services (SMS)	260.00
Total sold by managers to end users	81.00
Clicks number	12
Clicks amount	4.20\$
Impressions number	88
Impressions amount	1.76\$
It amount	1,154.04\$

Looking for a Captive Portal? Contact sales@fmsweb.de



MAC based PSK with Usermanager

- Separate PSKs per MAC
- Stored in Usermanager
- Easy to setup
- No full Radius necessary
- Enhanced security
- Access restrictions by device

A screenshot of the Mikrotik User Manager login interface. The page has a light green background with a dark grey header. The Mikrotik logo and 'Mikrotik User Manager' text are centered at the top. Below this, there are two input fields: 'Login' and 'Password'. A 'Log in' button is positioned below the password field.

- Configuration not nicely embedded in CAPsMAN concept



MAC based PSK with Usermanager

- Device wants to connect
- CAPsMAN sends MAC to Radius
- Radius returns personal PSK
- CAPsMAN compares PSK
- Grant or decline access

A screenshot of the MikroTik User Manager web interface. The page has a light green background with a dark grey header. The MikroTik logo and 'Mikrotik User Manager' text are centered at the top. Below this, there are two input fields: 'Login' and 'Password'. A 'Log in' button is positioned below the password field.



MAC based PSK: Radius

- Setup Radius connection
- Service
- IP Address
- Optional secret

#	Service	Called ID	Domain	Address	Secret
0	wireless			10.10.0.63	123

1 item (1 selected)

Radius Server <10.10.0.63>

General Status

Service: ppp login
 hotspot wireless
 dhcp

Called ID:

Domain:

Address: 10.10.0.63

Secret: 123

Authentication Port: 1812

Accounting Port: 1813

Timeout: 300 ms

Accounting Backup

Realm:

Src. Address: 0.0.0.0

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Status

enabled



MAC based PSK: CAPsMAN

The screenshot displays the CAPsMAN configuration interface with three key areas highlighted by red circles and arrows:

- 1** CAPs Security Configuration (wpa2security):
 - Name: wpa2security
 - Authentication Type: WPA PSK WPA2 PSK WPA EAP WPA2 EAP
 - Encryption: [empty]
 - Group Encryption: [empty]
 - Passphrase: [empty]
- 2** CAPs Access Rule configuration:
 - Action: query radius
- 3** CAPs AAA configuration:
 - MAC Format: XX:XX:XX:XX:XX:XX
 - MAC Mode: as username
 - MAC Caching: 00:00:10
 - Interim Update: [empty]

The background interface shows the 'Security Cfg.' tab selected, with a table listing interfaces (cap5, cap6) and a list of CAPs Access Rules.



MAC based PSK: Usermanager

Router details

▲ Main

Name: CAPsMAN-1

Owner: admin

IP address: 10.10.0.63

Shared secret: 123

Time zone: Parent time zone

Disabled:

Log events:

- Authorization success
- Authorization failure
- Accounting success
- Accounting failure

▼ Radius incoming

CoA support:

CoA port: 1700

▼ Request statistics

Save

User details

▲ Main

Username: 64:9A:BE:98:25:59

Password:

Disabled:

Owner: admin

▼ Actual profile

▼ Constraints

▲ Wireless

Preshared key: 87654321

Enc key:

Enc algo: AES-CCM

▼ Private information

▼ Statistics

▼ Bill

▼ All profiles

+ default

Save



WPA-Enterprise

CAPs Security Configuration <EAP-Passthrough>

Name: EAP-Passthrough

Authentication Type: WPA PSK WPA2 PSK WPA EAP WPA2 EAP ▲

Encryption: aes ccm tkip ▲

Group Encryption: [Dropdown]

Passphrase: [Text]

EAP Methods: passthrough [Dropdown]
EAP-TLS [Dropdown]

EAP Radius Accounting: passthrough [Dropdown]

TLS Mode: [Dropdown]

TLS Certificate: [Text]

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

Internally Supported

- EAP-TLS

Externally Supported

- all EAP methods
- passthrough



WPA-Enterprise related Terms

- 802.1X = 802 AA Standard

- EAP = Extensible

Authentication Protocol

- EAP-TLS

- EAP-TTLS

- PEAP (EAP-PEAP)

Protected Extensible

Authentication Protocol

- PEAPv0 with MSCHAPv2 often called PEAP





PEAP with MSCHAP

- Authenticate server by server side certificate
- Create TLS tunnel
- Create EAP session through encrypted tunnel
- Use EAP-MSCHAP for client authentication



- **WARNING:** not secure if server certificate isn't validated at client. MSCHAP isn't secure if fake AP can collect handshakes



Prepare CAPsManager for PEAP

CAPs Security Configuration <EAP-Passthrough>

Name: EAP-Passthrough

Authentication Type: WPA PSK WPA2 PSK WPA EAP WPA2 EAP ▲

Encryption: aes ccm tkip ▲

Group Encryption:

Passphrase:

EAP Methods: passthrough

EAP Radius Accounting:

TLS Mode:

TLS Certificate:

Radius

#	Service	Called ID	Domain	Address
0	wireless			10.10.0.
1	wireless			10.10.0.

Radius Server <10.10.0.108>

General Status

Service: ppp login hotspot wireless dhcp

Called ID:

Domain:

Address: 10.10.0.108

Secret: 123

Authentication Port: 1812

Accounting Port: 1813



RADIUS Server Selection

- No support in Usermanager
- Freeradius common choice
- Microsoft offers Radius

Zeroshell

- Ready to run appliance
- Linux based
- Includes Freeradius
- Includes certificate handling



www.zeroshell.org



Zeroshell Setup

- Download the image
- Install VM from CD image
- Change IP / set DHCP
- Change admin password

Default IP: 192.168.0.75

User: admin

Pass: zeroshell



www.zeroshell.org



Zeroshell Configuration

- Enable the Radius Server

The screenshot shows the Zeroshell Net Services interface. At the top, it displays the Zeroshell logo, version 3.5.0, and system status: Release 23.03 Kbit/s (Connections: 54 Load: 0%). There are links for About, Logout, Reboot, and Shutdown. A sidebar on the left contains a menu with SYSTEM (Setup, Logs, Utilities, Monitoring) and USERS (Users, Groups, RADIUS, Accounting). The main content area is titled 'RADIUS Server for Wireless and Identity Based Networking Services'. It shows the status as 'DOWN' and an unchecked 'Enabled' checkbox. Below this is the '802.1x Configuration' section, which includes an 'X.509 Host Certificate' dropdown set to 'Local CA' and 'OU=Hosts, CN=zeroshell.example.com', a 'View' button, and a status of 'OK'. A 'Check CRL' checkbox is also present. A red arrow points from the 'RADIUS' menu item in the sidebar to the 'Enabled' checkbox.



Zeroshell Configuration

- Add an authorised client

RADIUS AUTHORIZED CLIENTS

Client Name IP or Subnet / Shared Secret

	Client Name	IP or Subnet	Shared Secret
<input type="radio"/>	CAPsMAN-1	10.10.0.63	123



Zeroshell Configuration

- Add an user account

1

USERS List View Add Edit Delete X509 Kerberos 5

Alerts: **None**

John Testuser (capsuser) **3** Submit Reset

2

Account Information

Username capsuser UID Primary Group nobody GID 65534

Home Directory /home/capsuser Default Shell bash sh tcsh other /bin/false

User Information

Firstname John Lastname Testuser Organization ?

Description John Testuser E-Mail ? Phone ?

RADIUS Accounting

Expiration (mm/dd/yyyy) / /

Accounting Class DEFAULT

Credit: 0.00 € + Limits Costs (postpaid)

- MB - h - Mb/s 0.00€/MB 0.00€/h

User Password

Password

Confirm

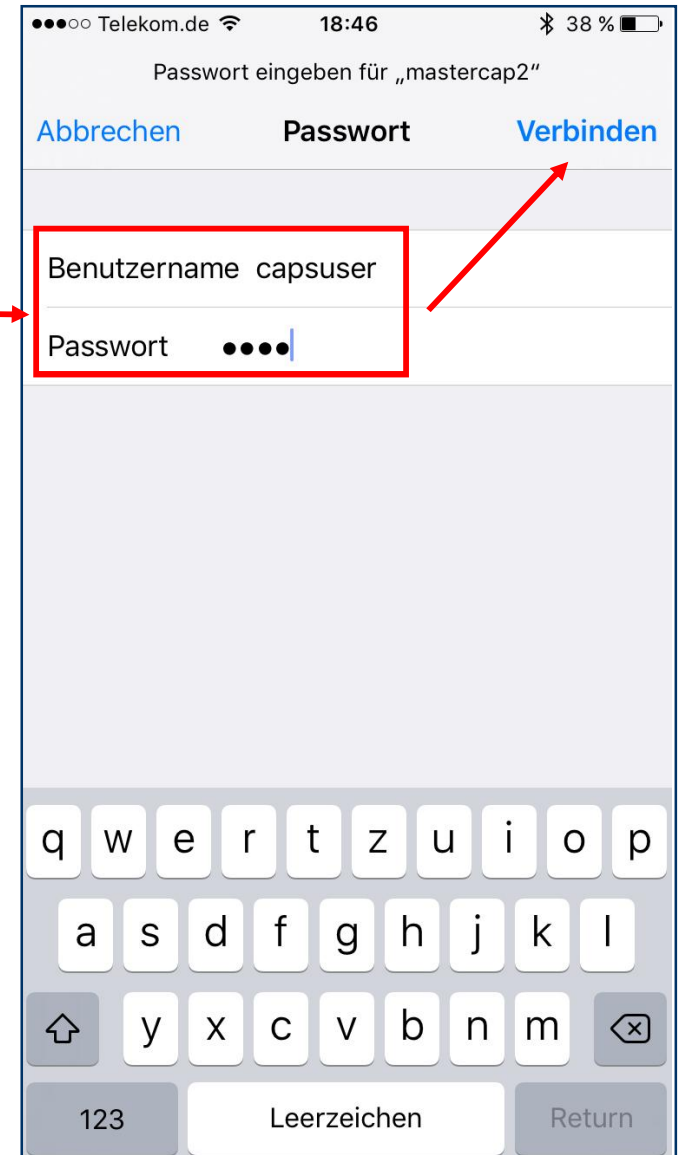
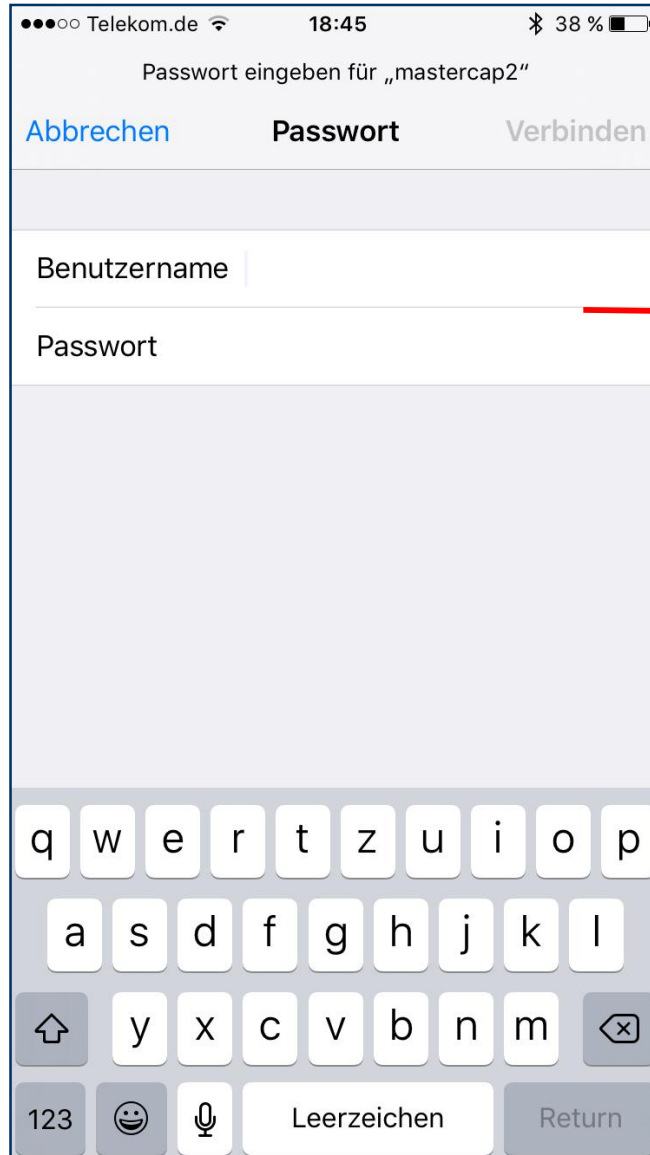
Authentication Protocol

Kerberos 5

RADIUS (VLAN)

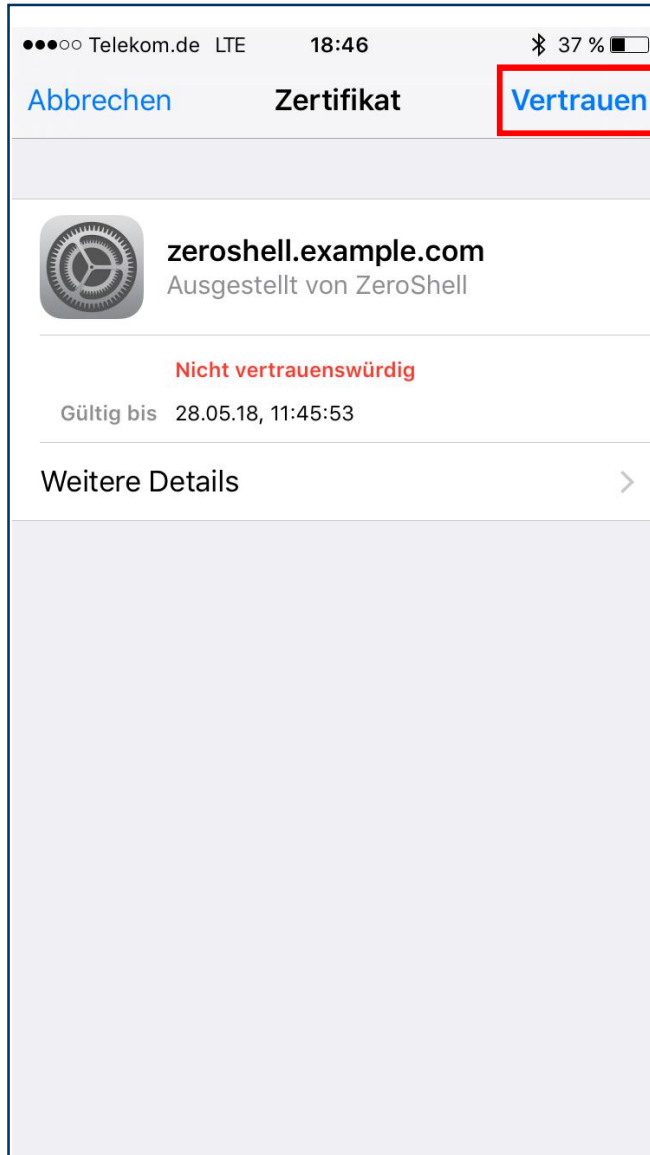


Connect an iPhone with PEAP





Connect an iPhone with PEAP





THANK YOU

... and enjoy the Usermeeting



FMS Internetservice GmbH

Phone: +49 761 2926500

Web: www.fmsweb.de

Shop: www.mikrotik-shop.de

Email: sales@fmsweb.de

Twitter: https://twitter.com/fmsweb_de