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

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

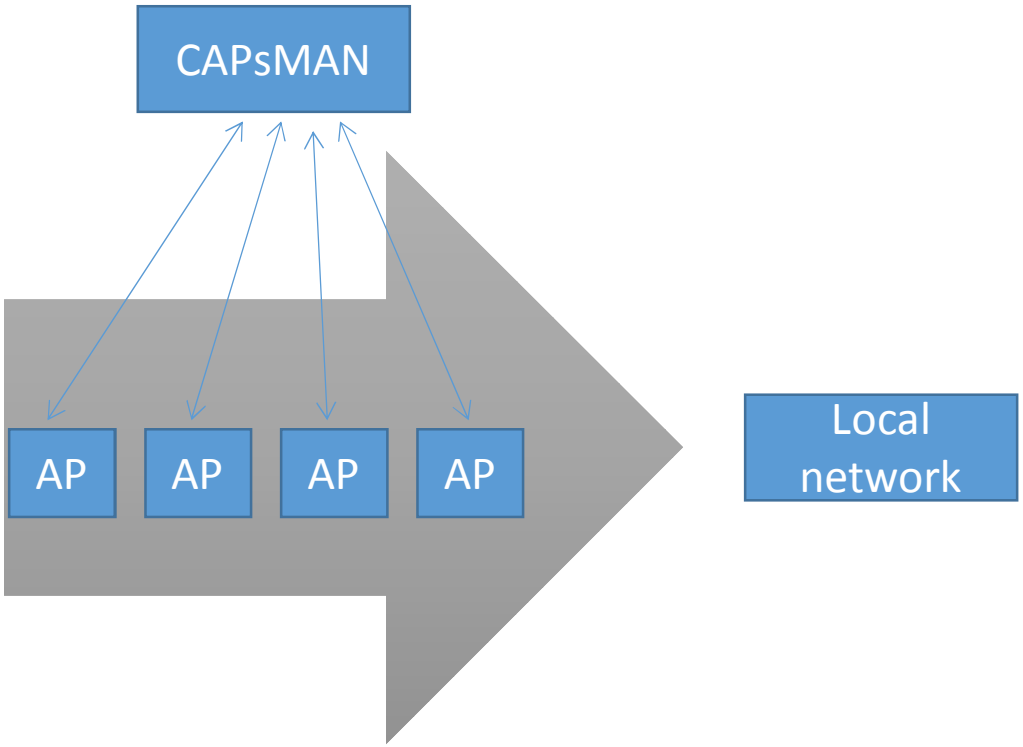
What is it about and how to get it running

CAPsMAN Basic Features

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

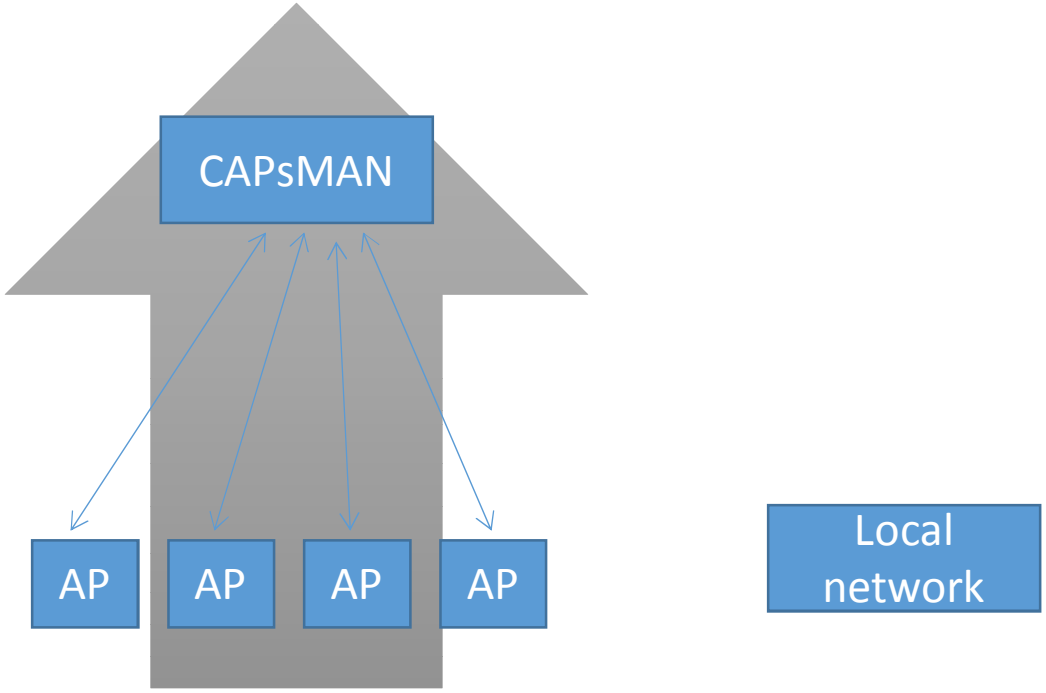
Client Traffic: Local Forwarding

- Access point handles traffic
- Manual access point configuration



Manager Forwarding

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

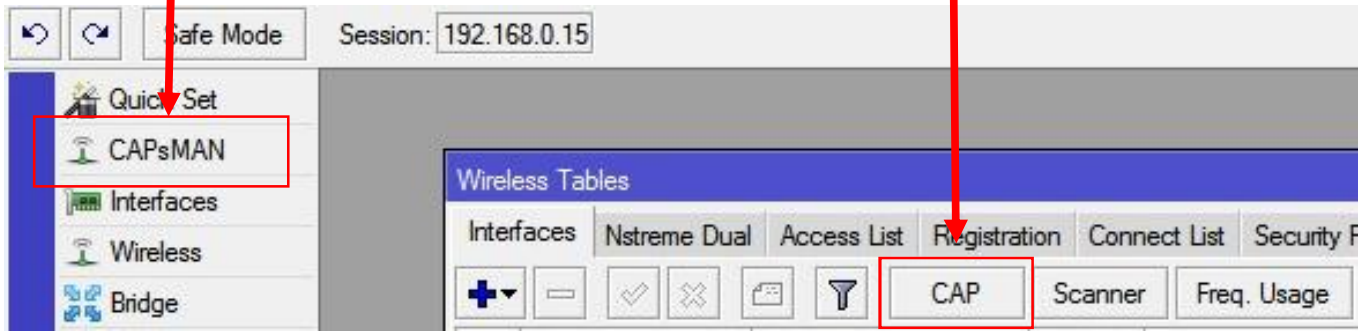


Getting Started

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

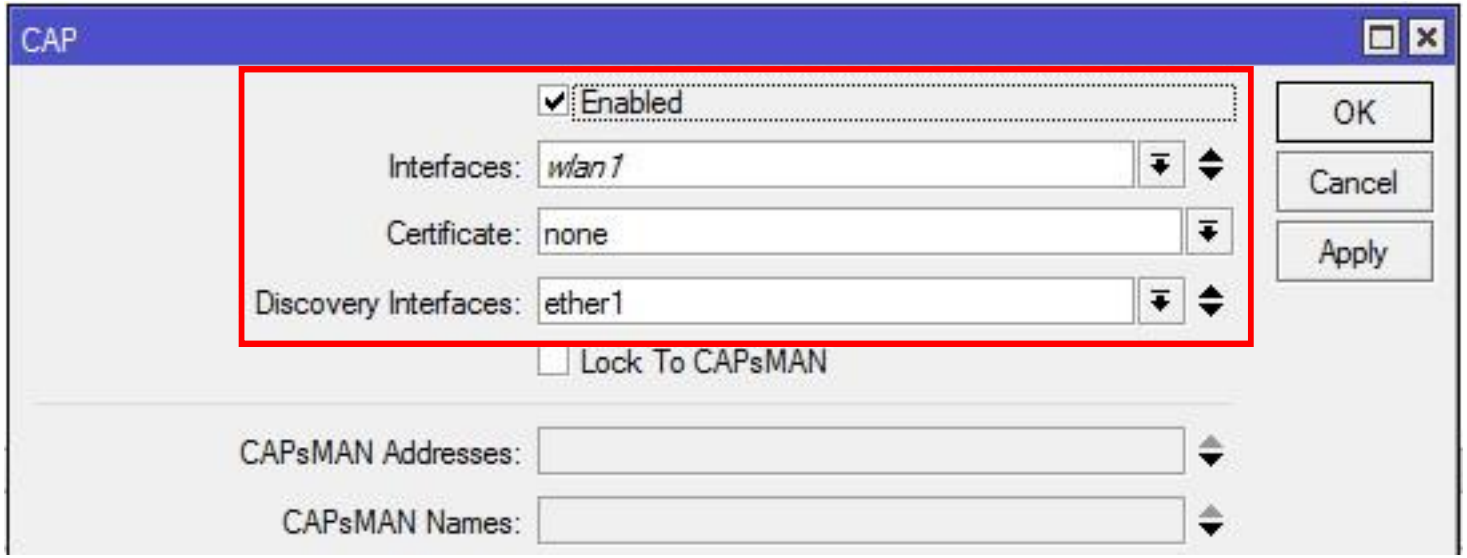
CAPsMAN configuration

CAP configuration

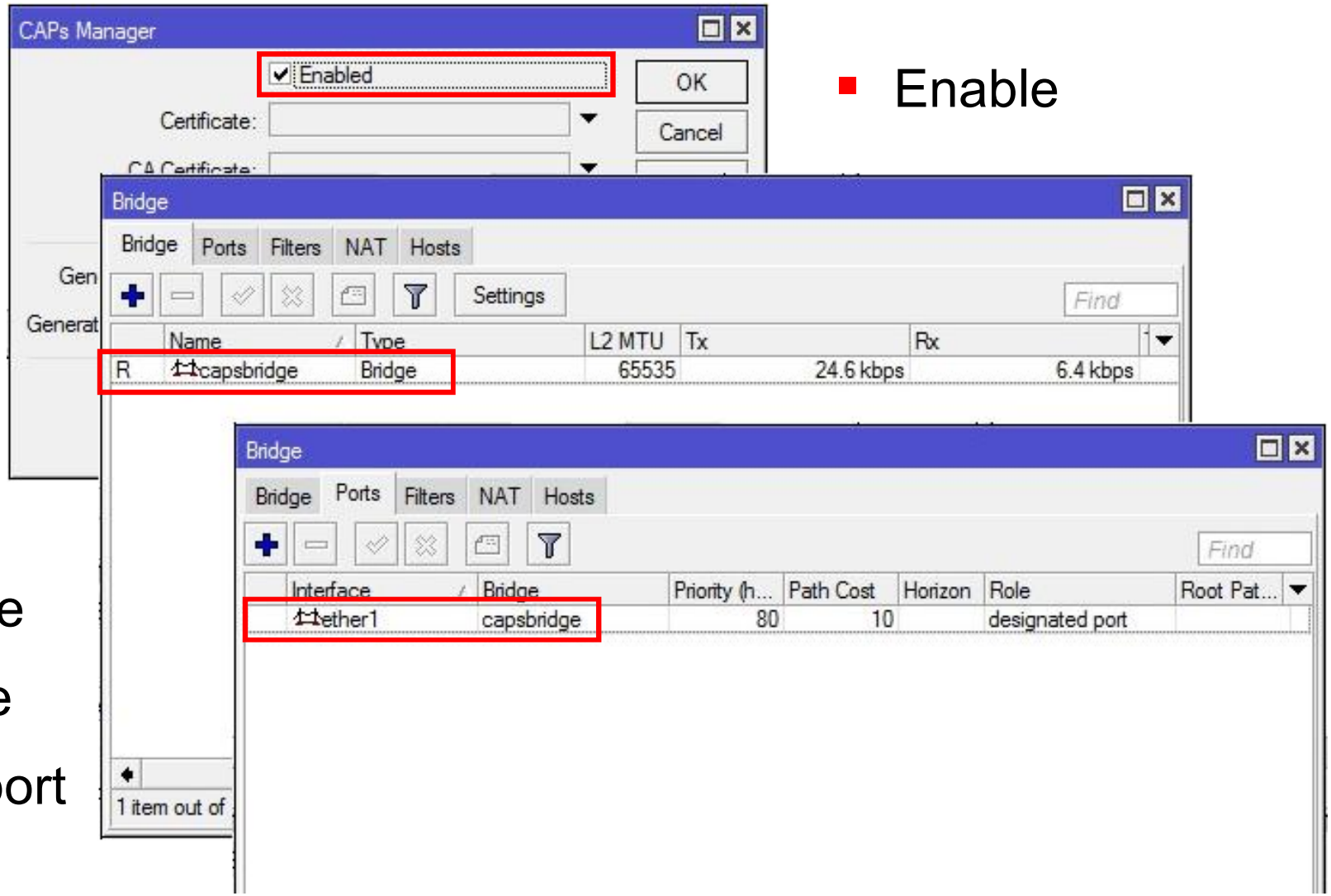


Minimum CAP Configuration (Layer 2)

- Enable
- Choose CAP interfaces
- Choose discovery interfaces

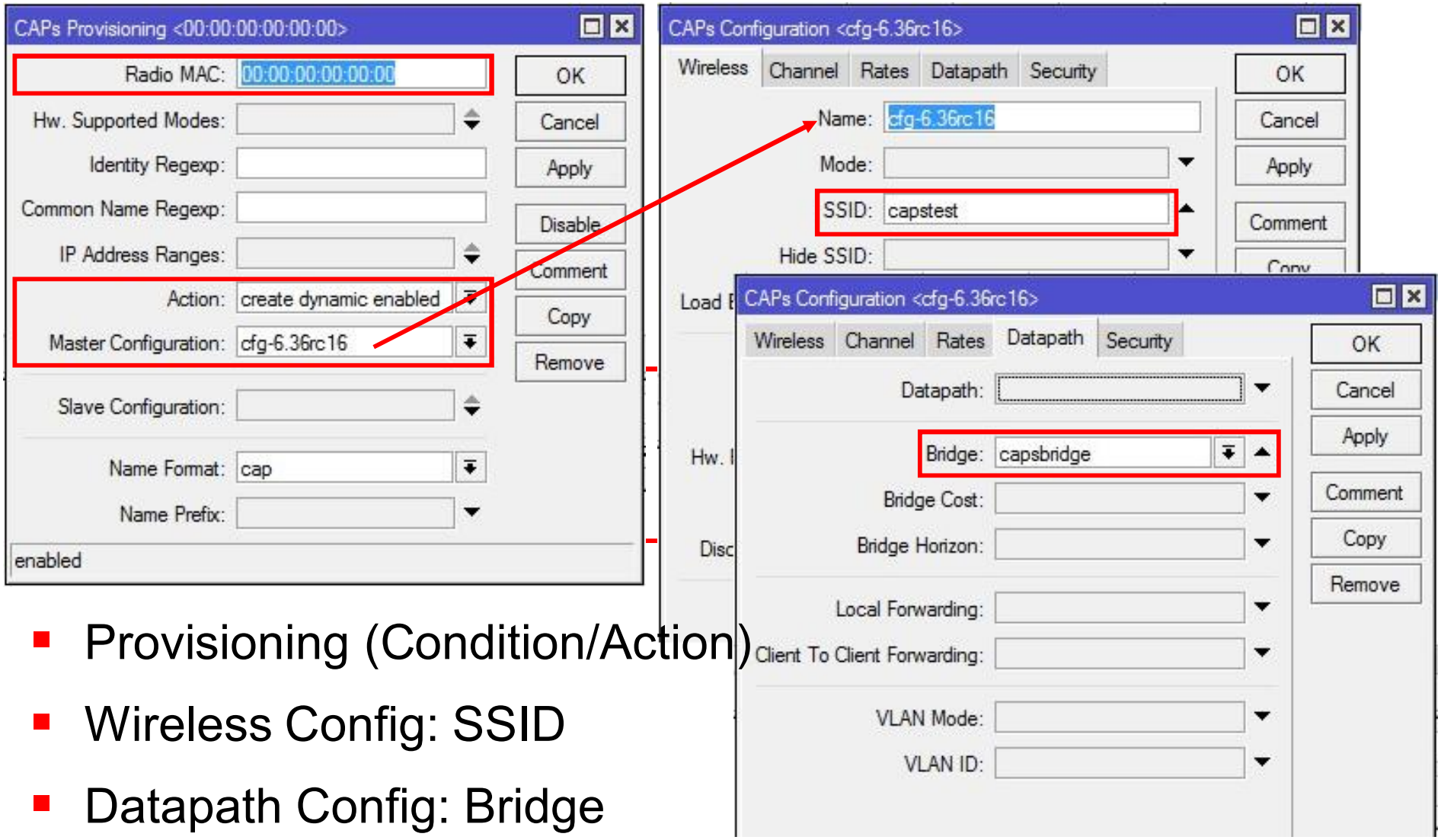


Minimum CAPsMAN Configuration



- Enable
- Create bridge
- Add port

Minimum CAPsMAN Configuration



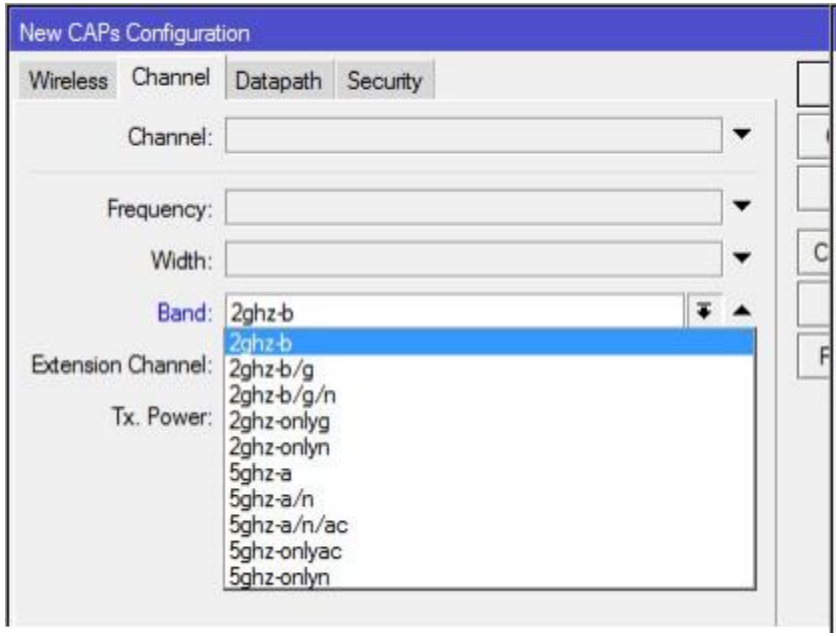
- Provisioning (Condition/Action)
- Wireless Config: SSID
- Datapath Config: Bridge

Latest CAPsMAN Features

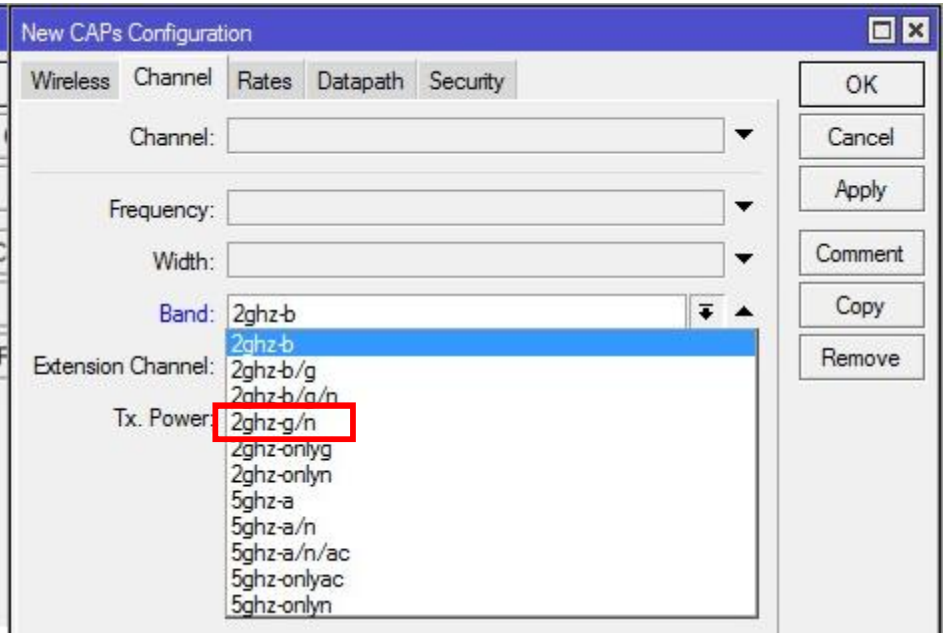
See what’s new

Changes wireless-rep Package

wireless-cm2



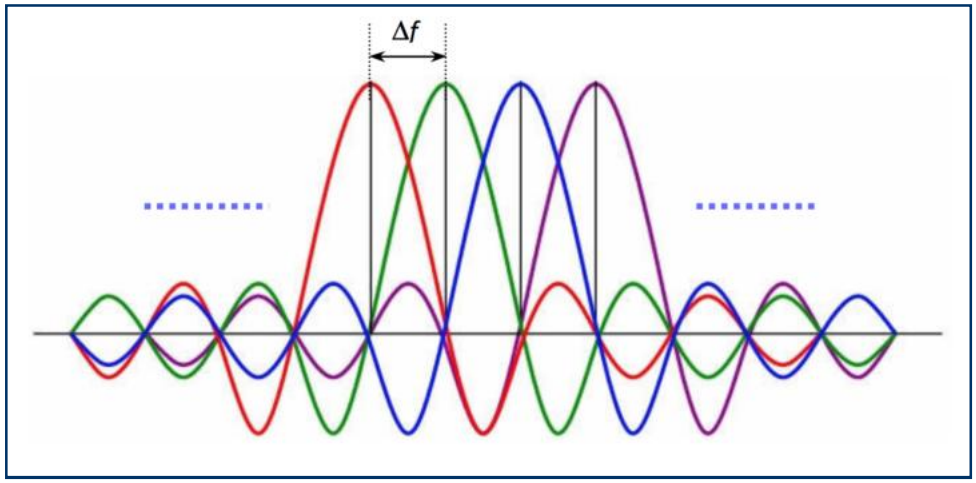
wireless (formerly wireless-rep)



- Optimize 2.4GHz performance
- Disable 802.11b legacy mode

Optimize performance w/o 802.11b

- 802.11b uses DSSS modulation

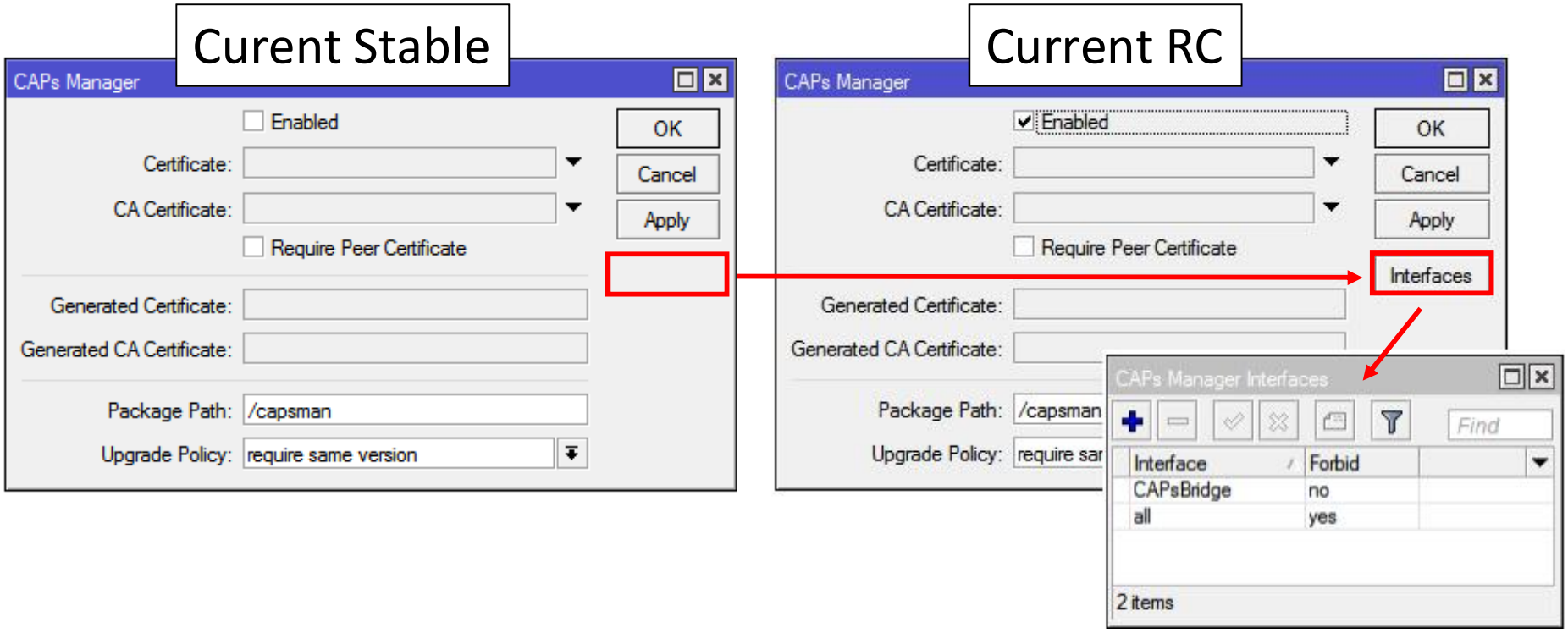


- 802.11g/n uses OFDM modulation

- OFDM node have to take care on DSSS nodes
- DSSS nodes use more air time

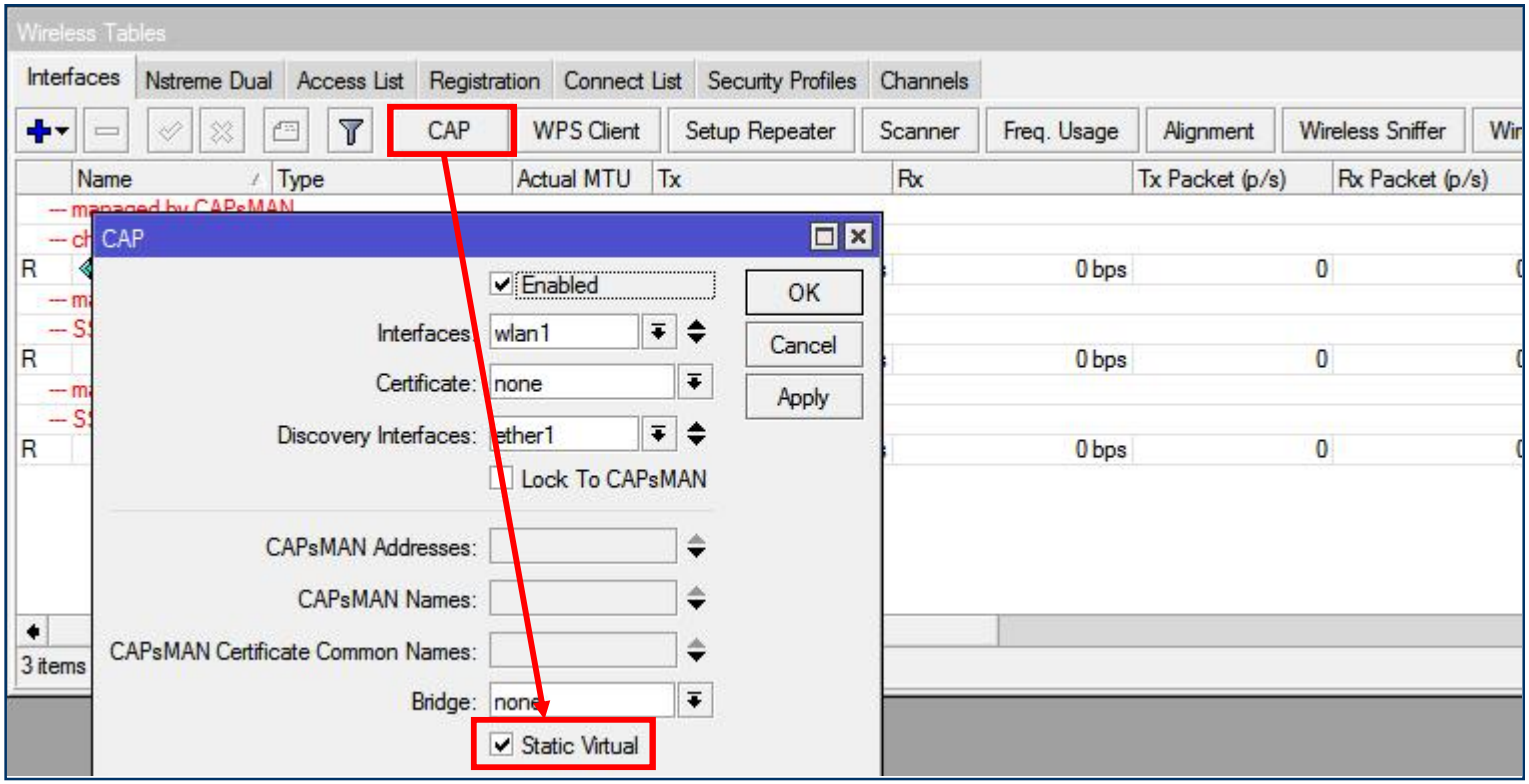
Latest Changes: Discovery Interface

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



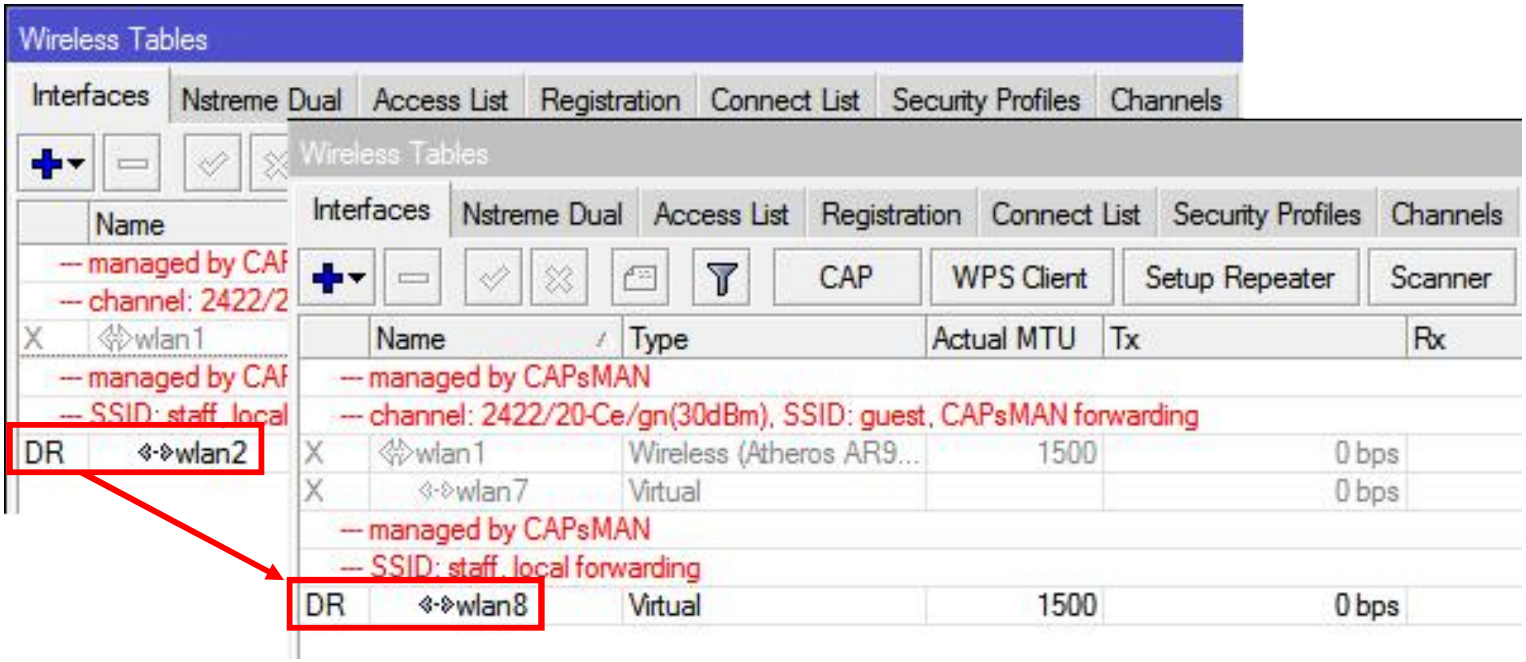
Latest Changes: Static Virtual

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



Latest Changes: Static Virtual

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



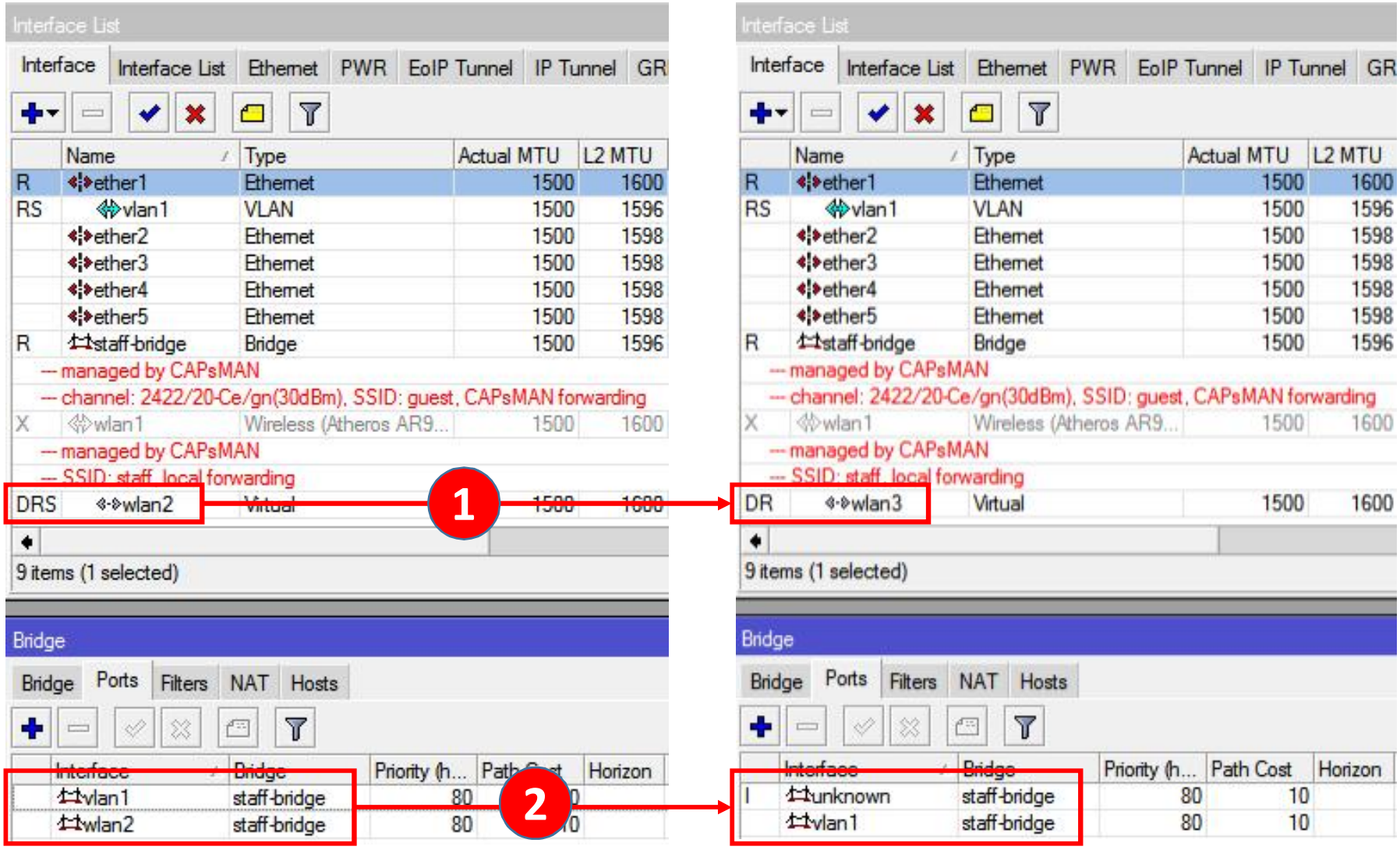
Latest Changes: Static Virtual

- Local forwarding: enabled interface
- Local interface configuration necessary

- E.g. local traffic handling:

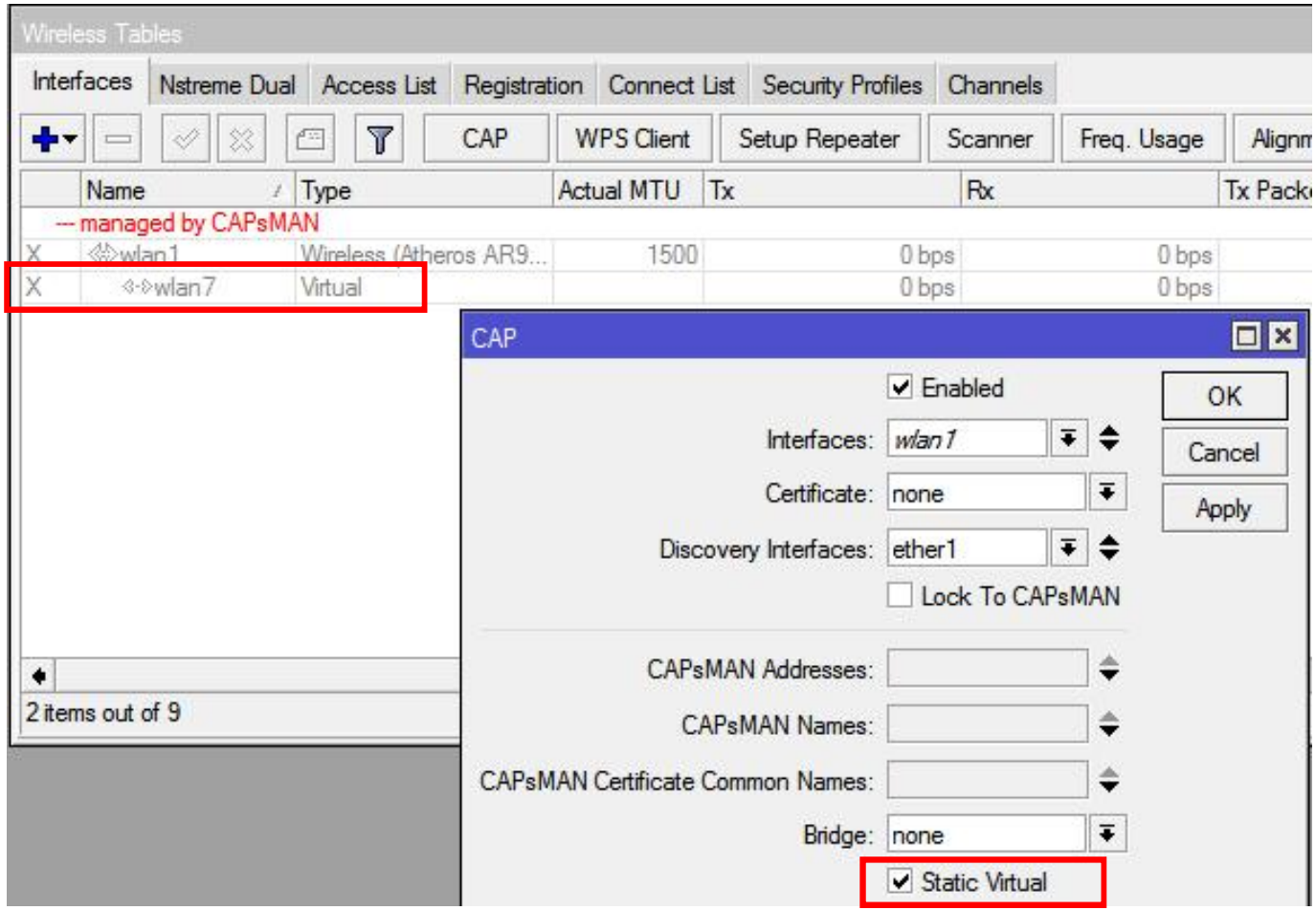
- Forwarding traffic to VLAN
- By using virtual interface as bridge port

Latest Changes: Static Virtual



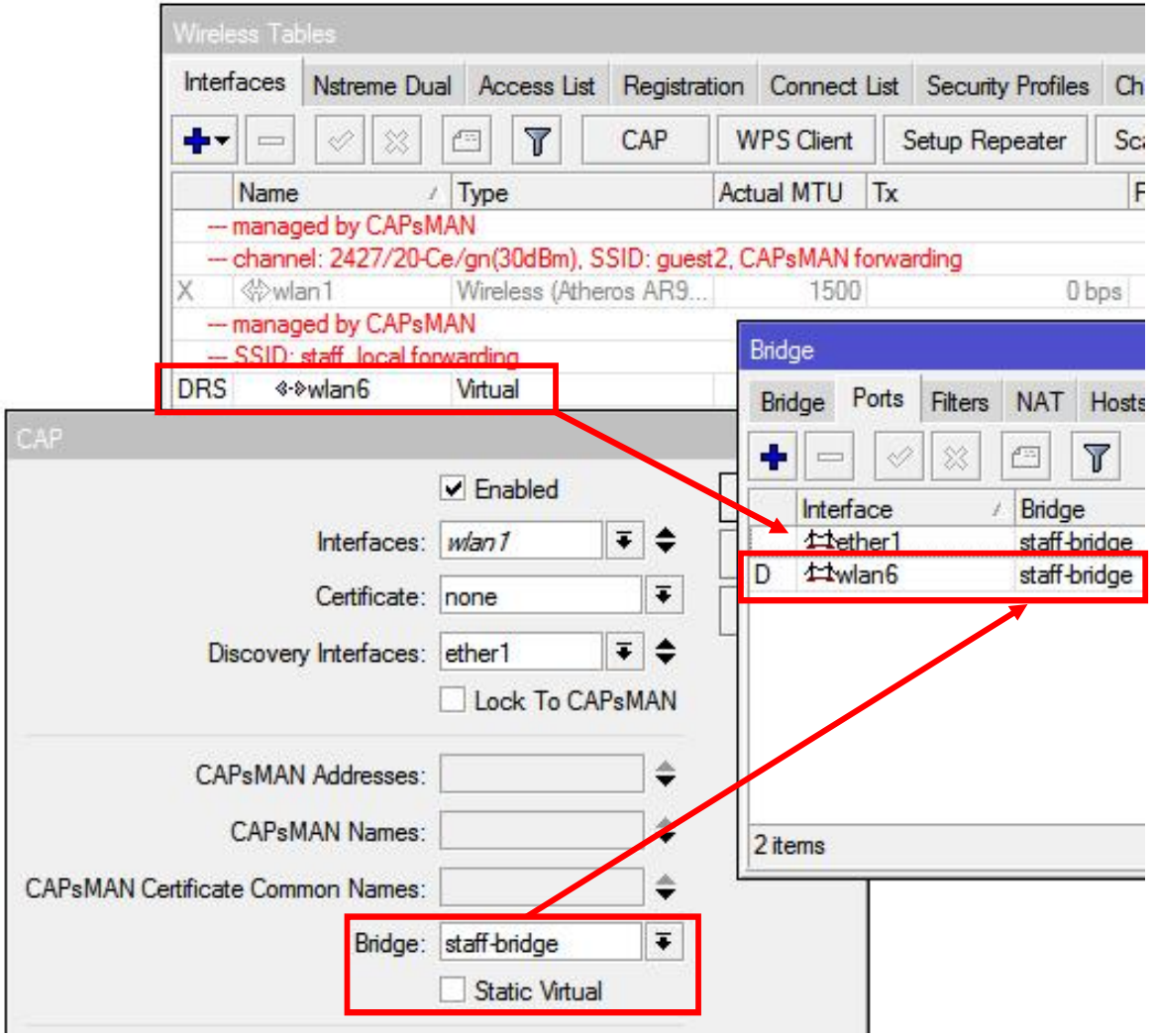
Latest Changes: Static Virtual

- wlan7 just disabled, not removed



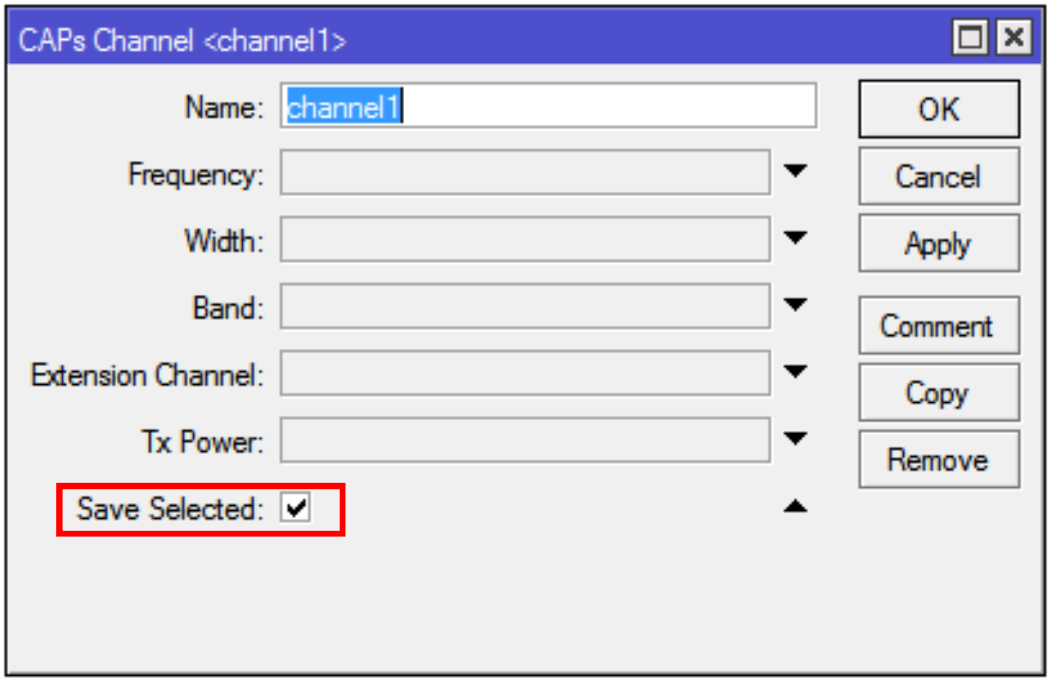
Static Virtual vs. CAP Bridge Setting

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

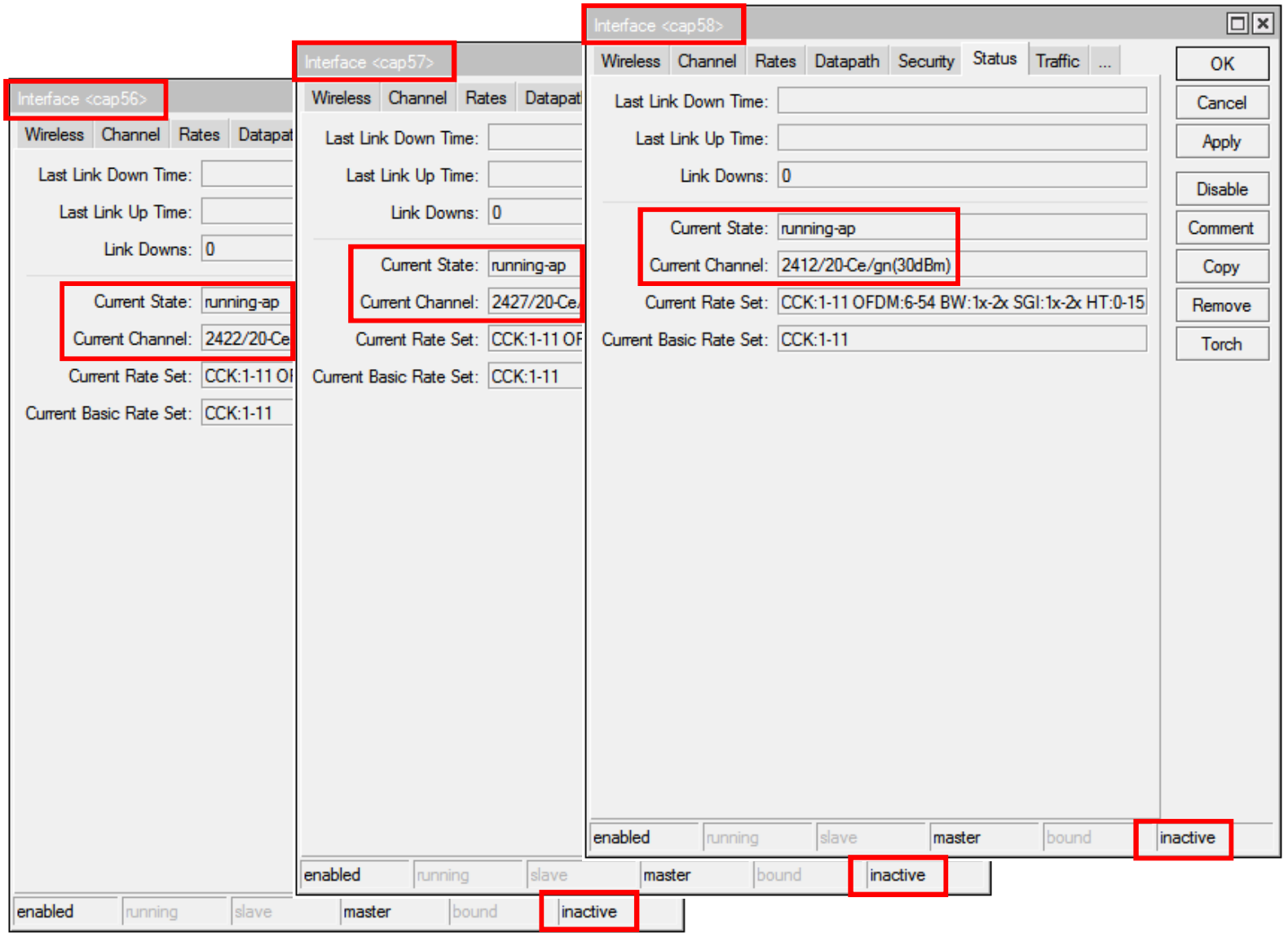


Latest Changes: Save Selected

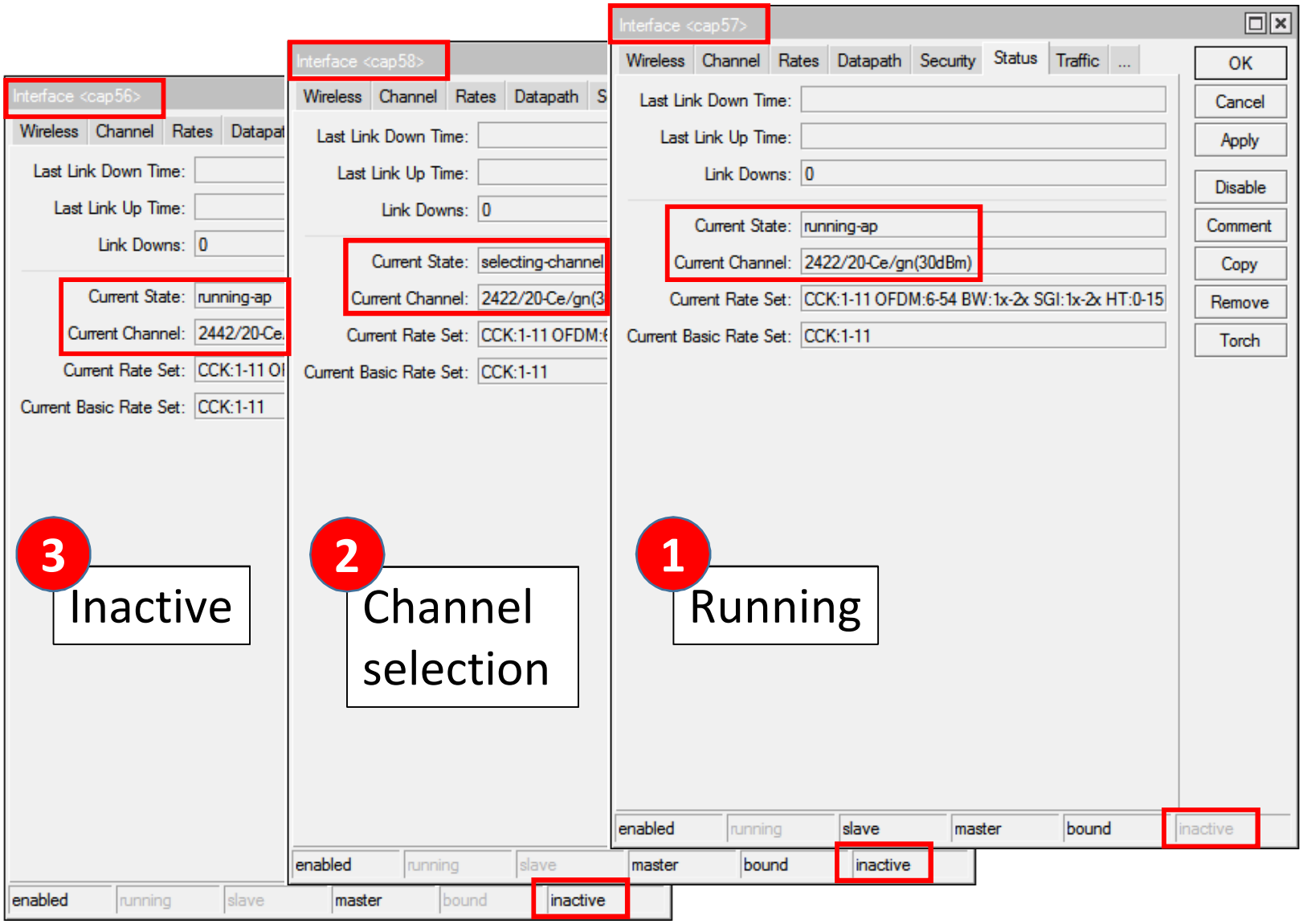
- Save selected channel
- No frequency set = “auto”
- Speeds up frequency selection on CAPsMAN start



Save Selected: CAPsMAN Disabled



Save Selected: CAPsMAN Reconnect



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

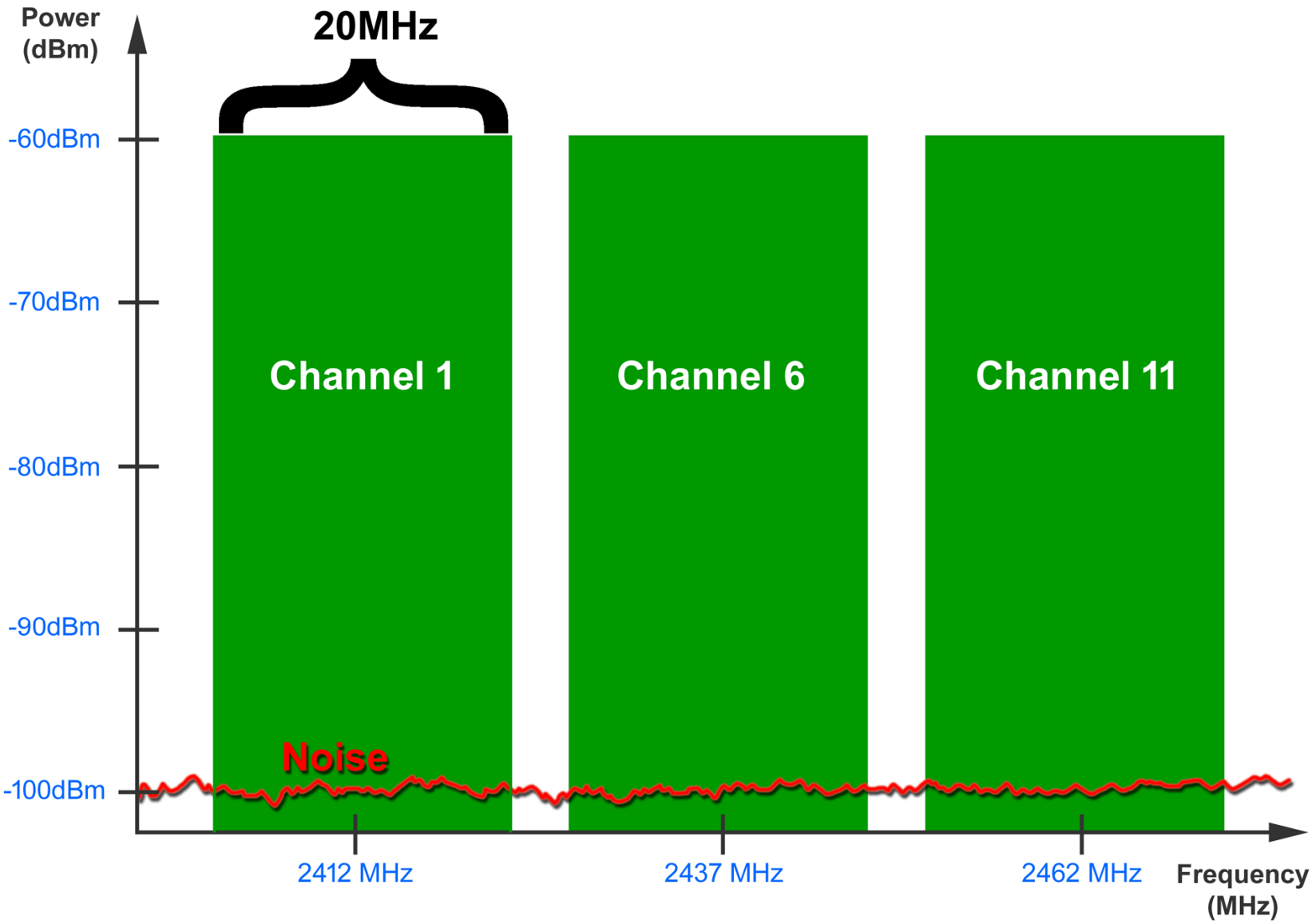
2,4GHz Channel Planning

- No channel 12/13 with FCC devices
- Public WiFi limited to channel 1 – 11

- Non overlapping channels: 1,6,11

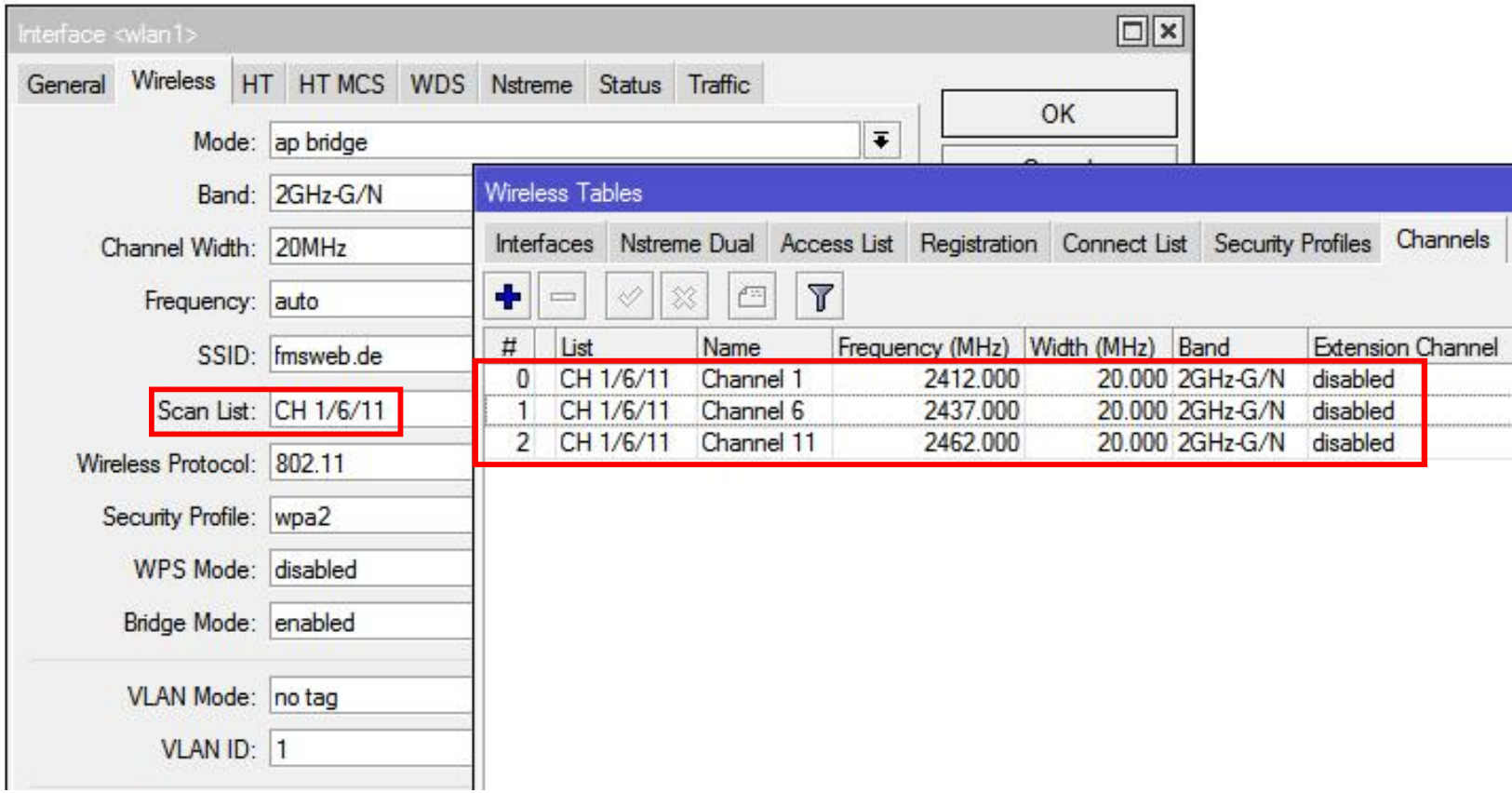
Channel	ETSI	FCC
1	**20dBm**	**30dBm**
2	20dBm	30dBm
3	20dBm	30dBm
4	20dBm	30dBm
5	20dBm	30dBm
6	**20dBm**	**30dBm**
7	20dBm	30dBm
8	20dBm	30dBm
9	20dBm	30dBm
10	20dBm	30dBm
11	**20dBm**	**30dBm**
12	20dBm	n/a
13	20dBm	n/a

2,4GHz Channel Planning



2,4GHz Channel Planning

- Without CAPsMAN: Use Scan List & Channels



2,4GHz Channel Planning

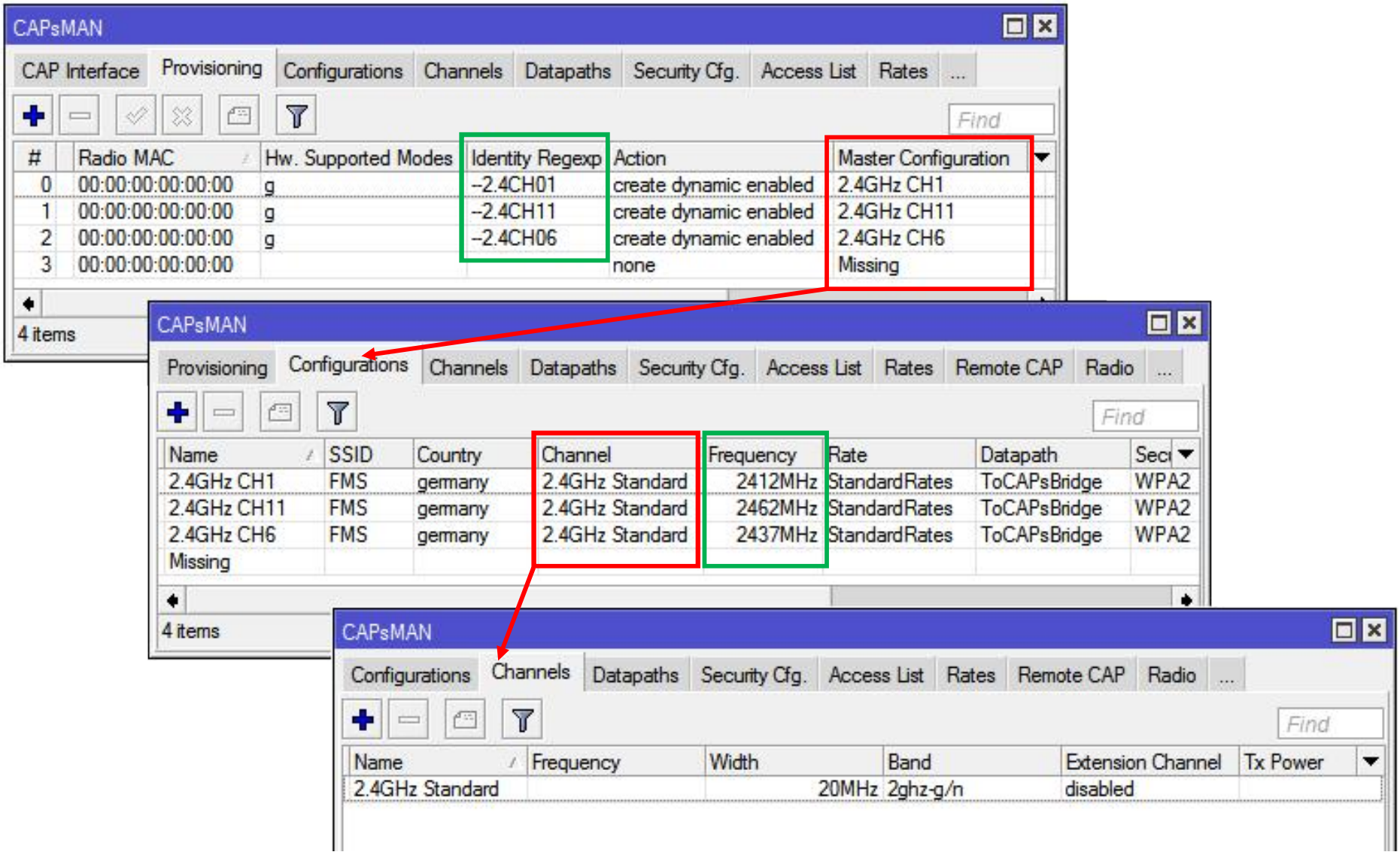
- Problem: No scan list option in CAPsMAN

- Configure CAPsMAN interfaces one by one?
- Controller advantage reduced

- Work around using CAPsMAN strengths
- Provisioning rules
- Modular hierarchical configuration

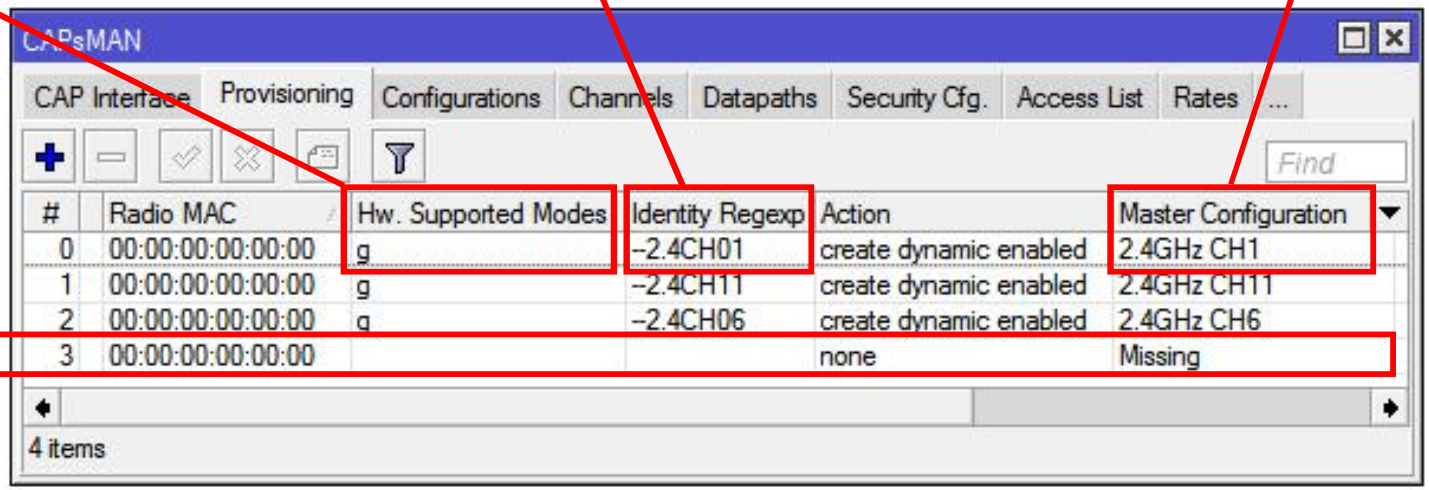
- RegEx and Overrides

Channel 1-6-11 Setup



Channel 1-6-11 Setup

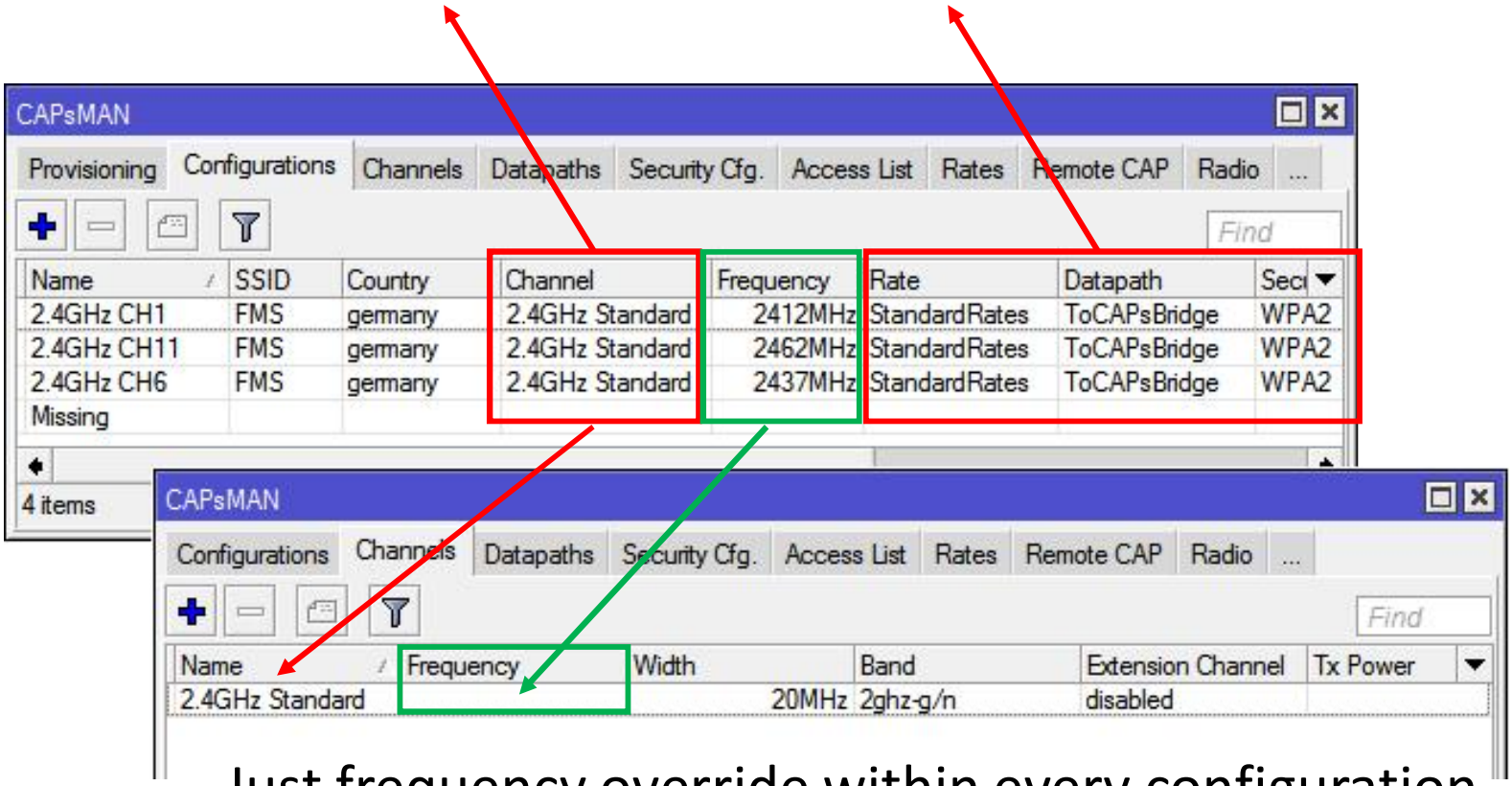
1. Require 802.11g, no Legacy support
2. Check CAP identity by RegEx for wanted channel
3. Use configuration according to RegEx



4. Catch-All Rule | Avoids static interface creation
   Find unwanted and misconfigured CAP (802.11b or identity not set)

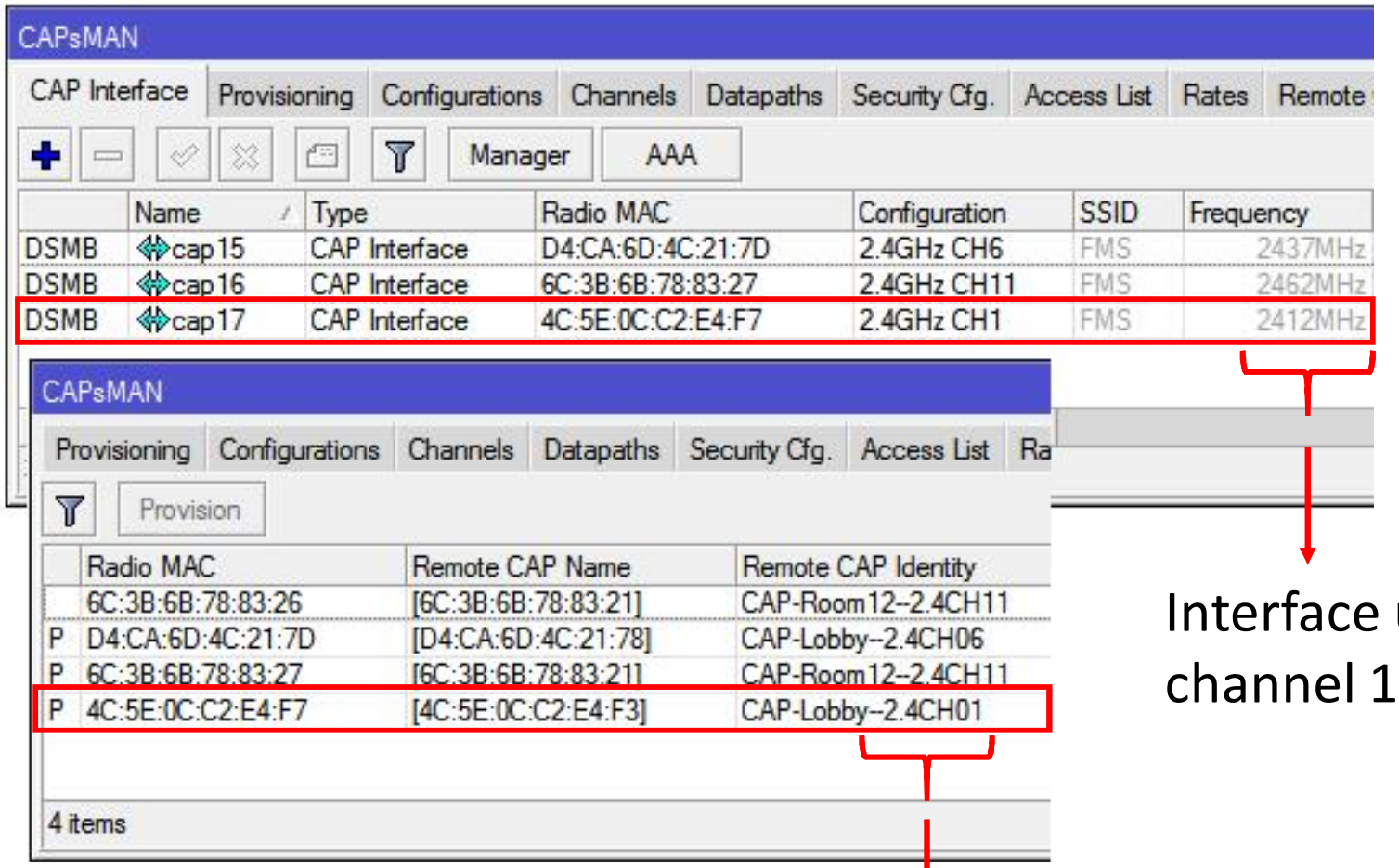
Channel 1-6-11 Setup

Common central setting blocks for maximum modularity



Just frequency override within every configuration

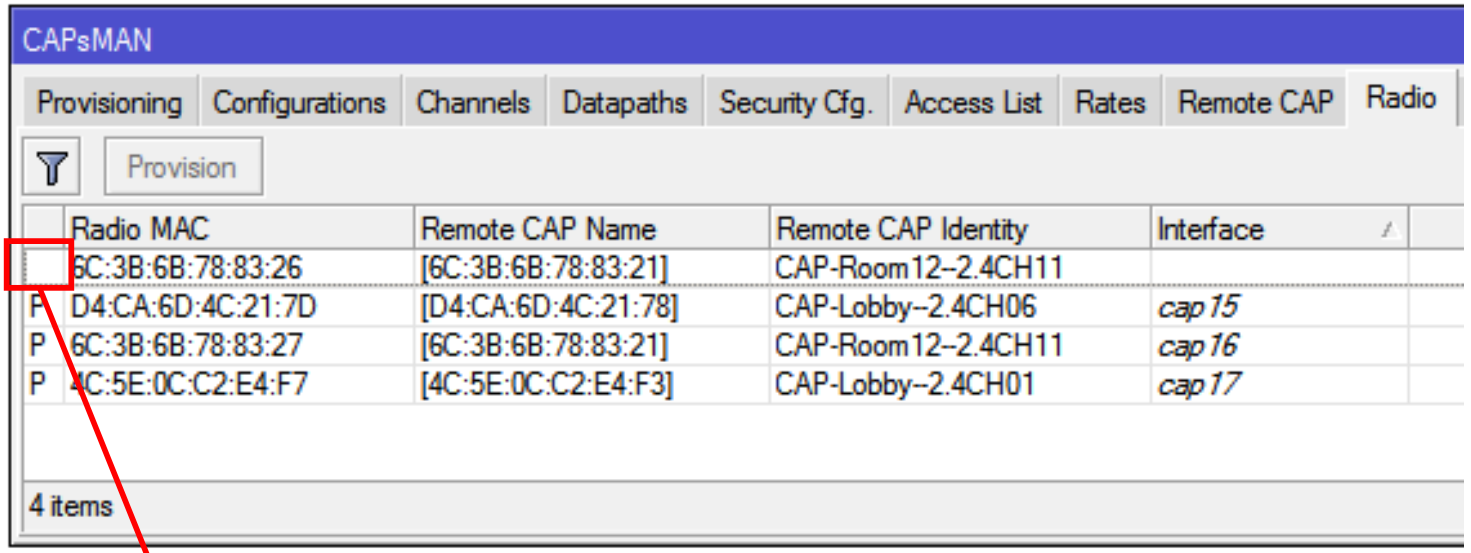
Channel 1-6-11 Setup



Interface uses channel 1 (2412MHz)

Identity contains „--2.4CH01“

Channel 1-6-11 Setup



Interface not provisioned

Catch all rule | Action = none

Reason: not supporting 802.11g

5GHz Regulation

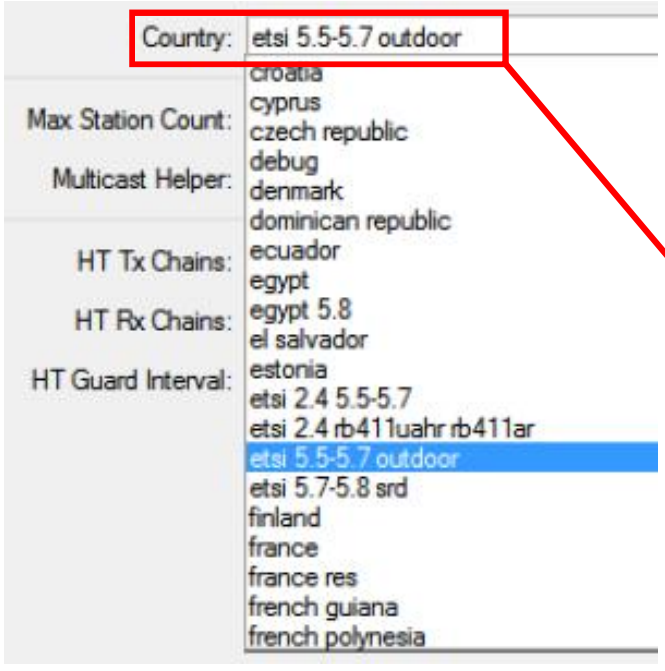
- Radar detection / DFS
- Not yet possible with CAPsMAN

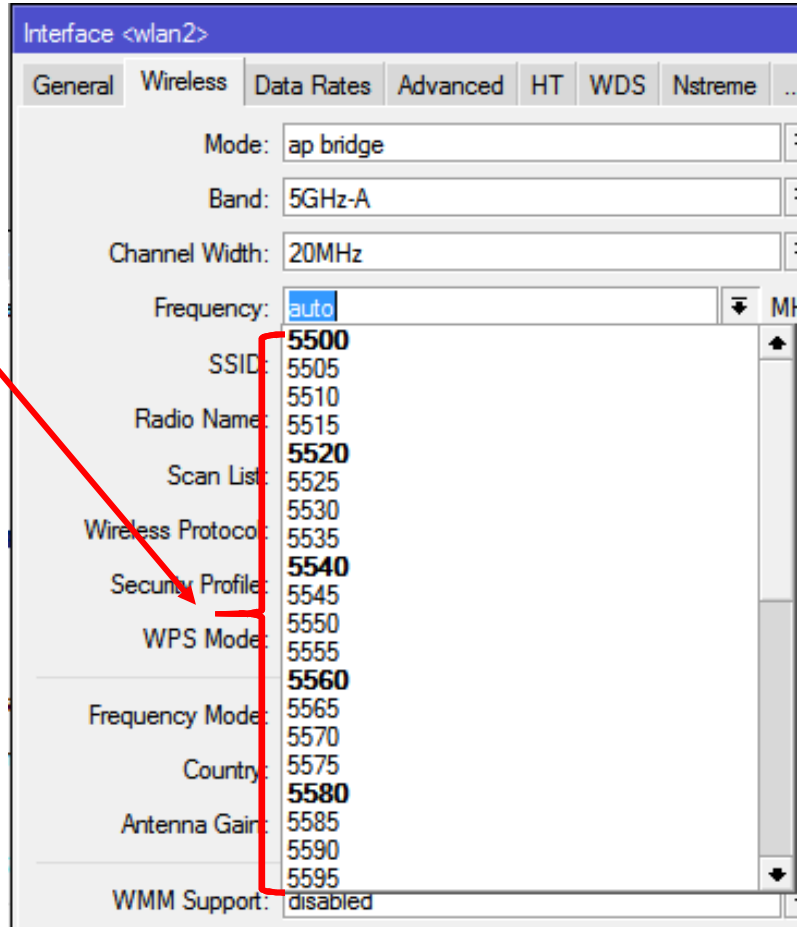
- Is currently being implemented

- Frequencies < 5470 MHz only indoor
- Outdoor setups without scan list?

5GHz Outdoor Channels

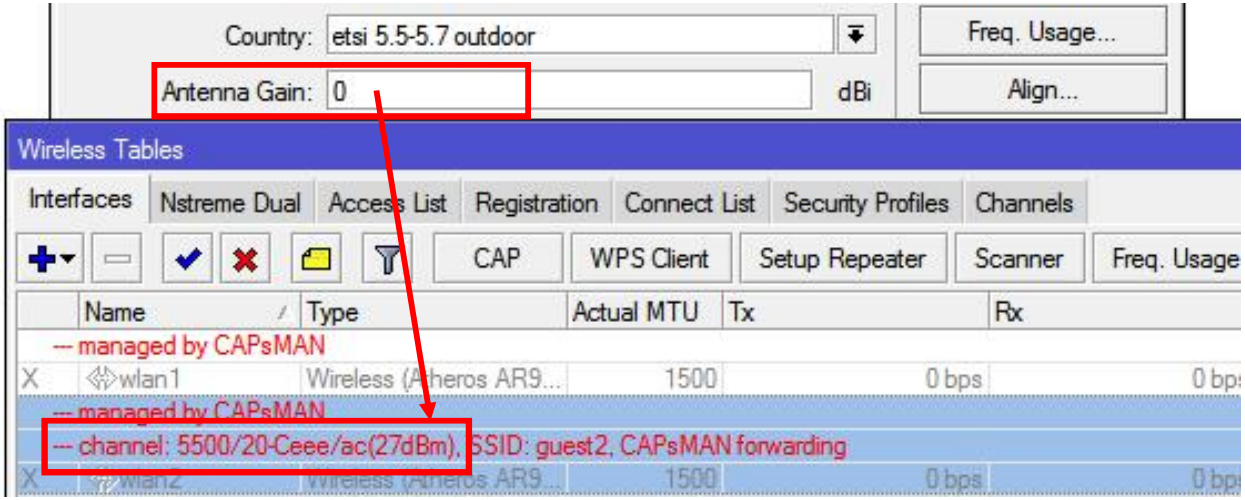
- Solution: etsi 5.5 – 5.7 outdoor





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



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

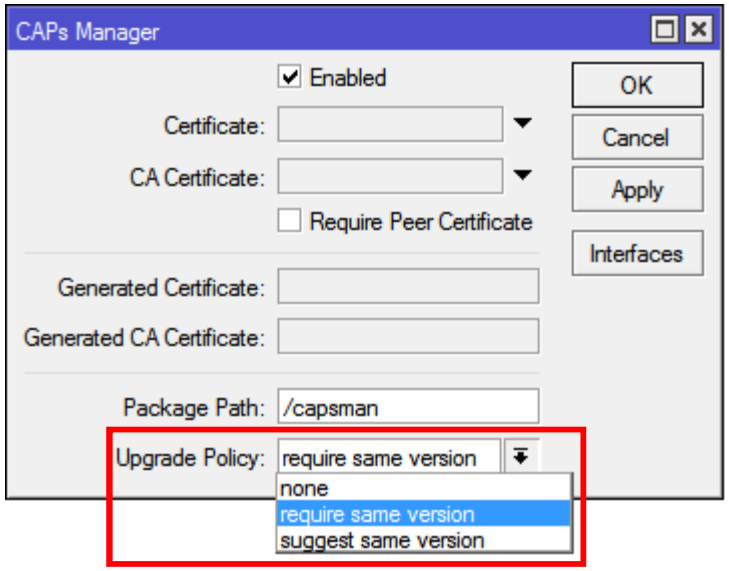
- iPhone 5 ~ 12dBm Tx, -0,8dBi = 11,2dBm EIRP

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

```
: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
4C:5E:0C:C2:E4:F3/4/c921 failed to connect, timeout
```

4

```
:5E:0C:C2:E4:F3/4/3598,Run,[4C:5E:0C:C2:E4:F3]] removed by user request
:5E:0C:C2:E4:F3/4/91da,Join,[4C:5E:0C:C2:E4:F3] joined, provides radio(s): 4C:5E:0C:C2:E4:F7
: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

Backup | Restore | Upload... | Find

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

5 items | 40.1 MiB of 63.8 MiB used | 37% free

CAPs Manager

Enabled

Certificate:

CA Certificate:

Require Peer Certificate

Generated Certificate:

Generated CA Certificate:

Package Path: /capsman

Upgrade Policy: require same version

OK | Cancel | Apply | Interfaces

WIFI Security

Security types supported by CAPsMAN

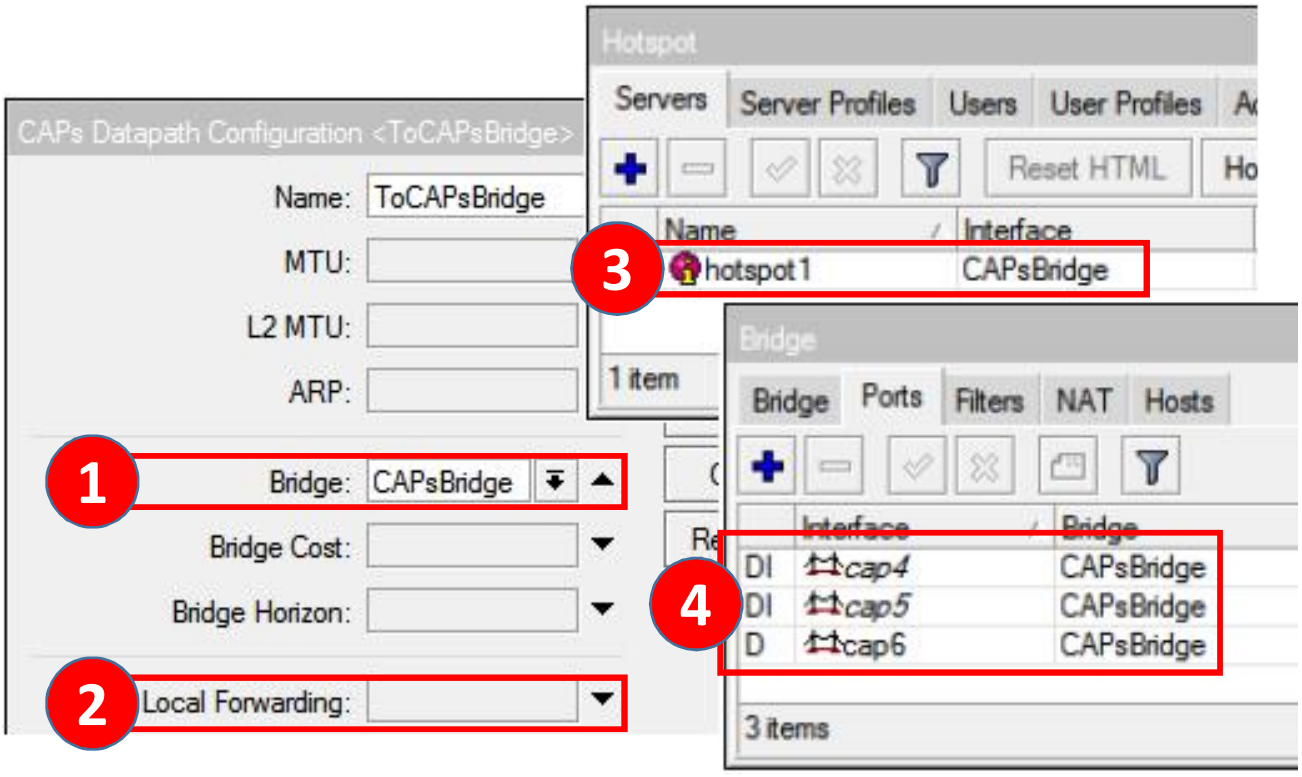
Security Overview

- 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



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

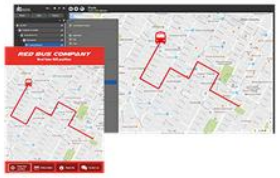
HS Network Manager

Responsive login

Social login

Payment options

Redundancy,
load balancing



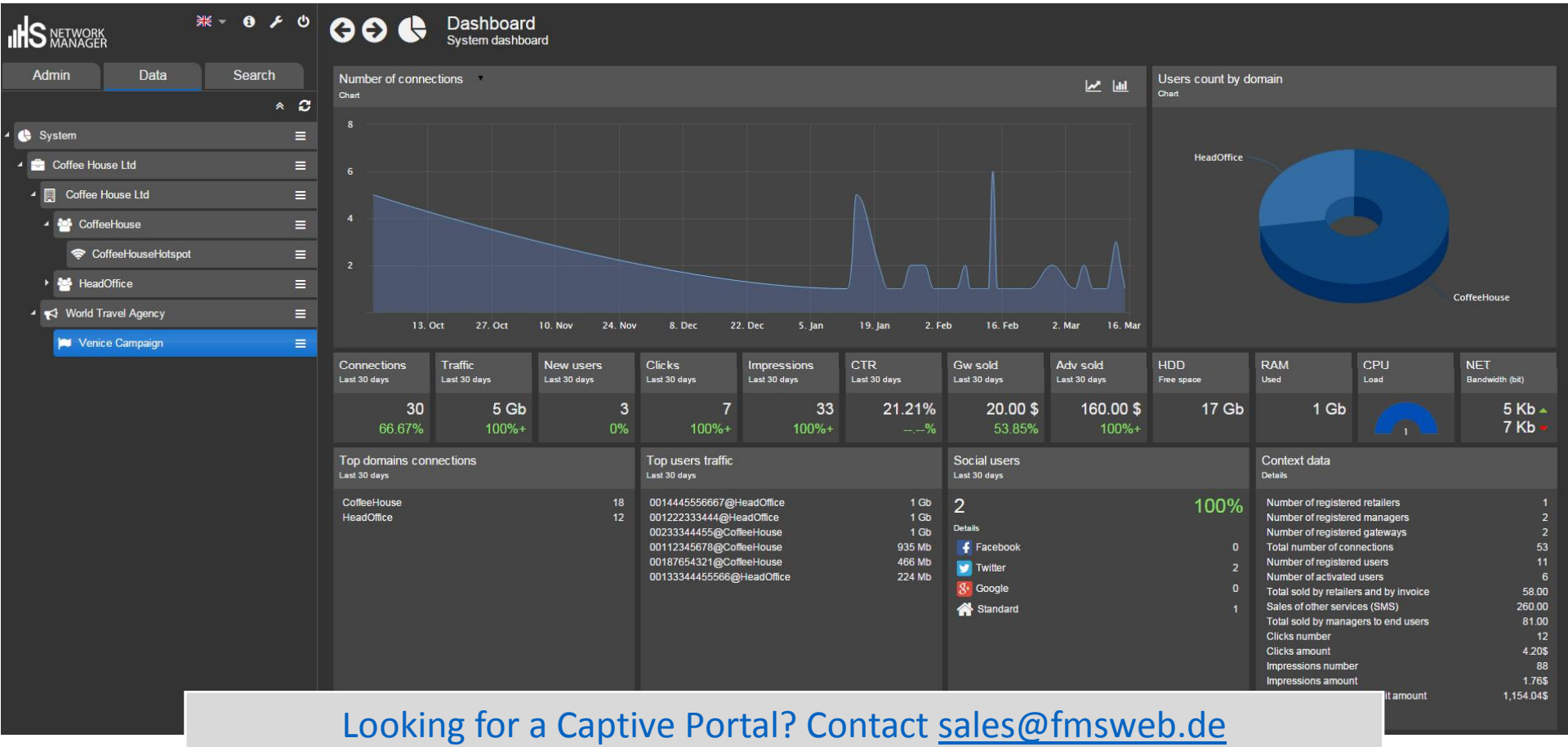
GPS tracking
(e.g coaches)

SMS authentication

Ticket printer

Advertising, surveys,
quizzes

HS Network Manager



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

- Configuration not nicely embedded in CAPsMAN concept

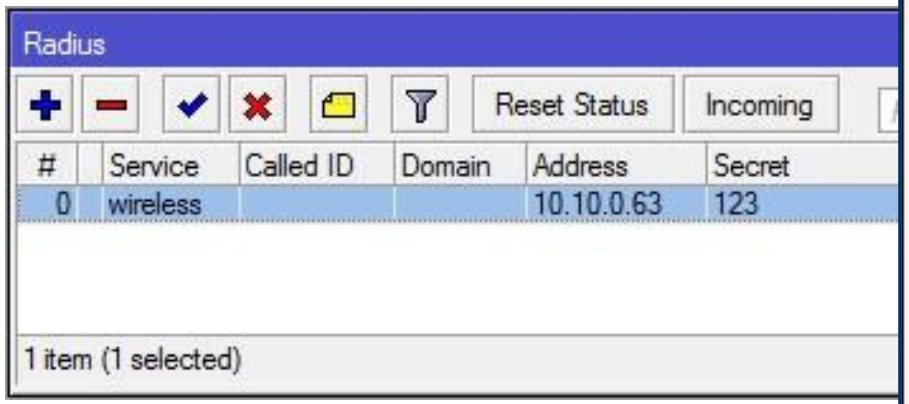
MAC based PSK with Usermanager

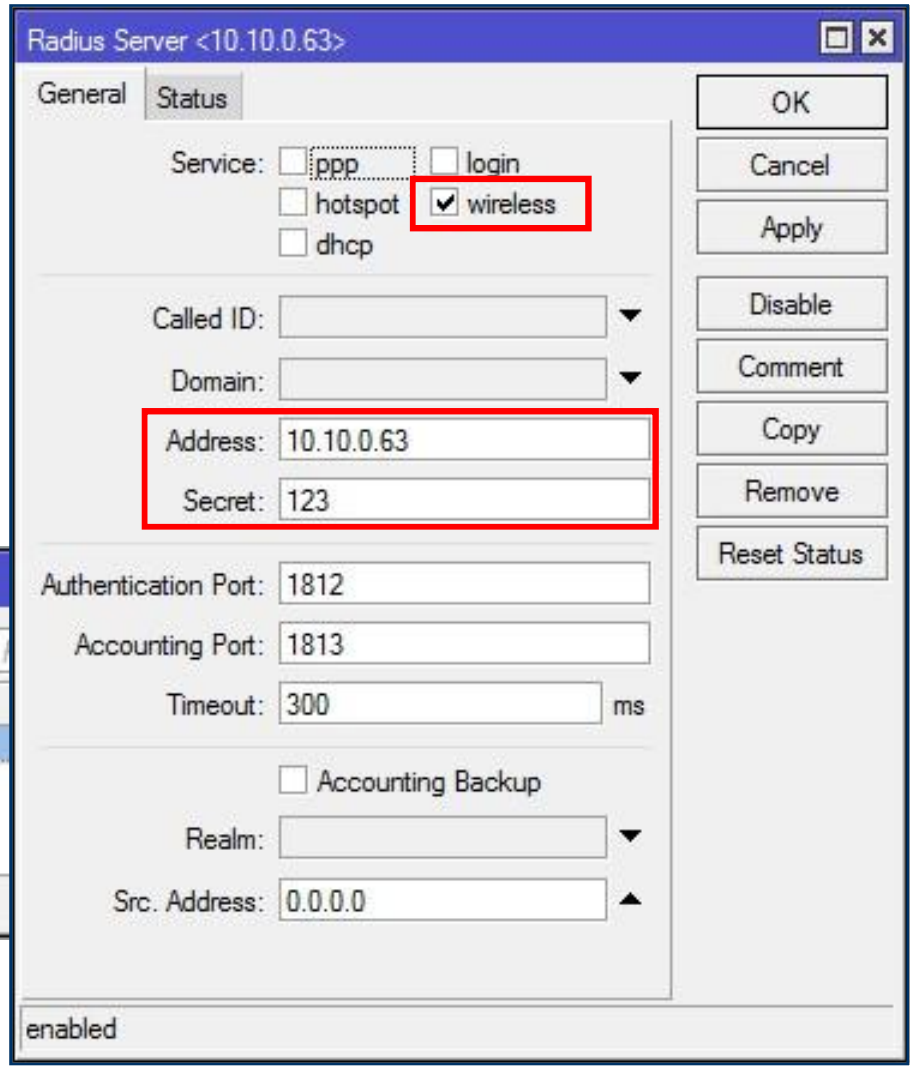
- Device wants to connect
- CAPsMAN sends MAC to Radius
- Radius returns personal PSK
- CAPsMAN compares PSK

- Grant or decline access

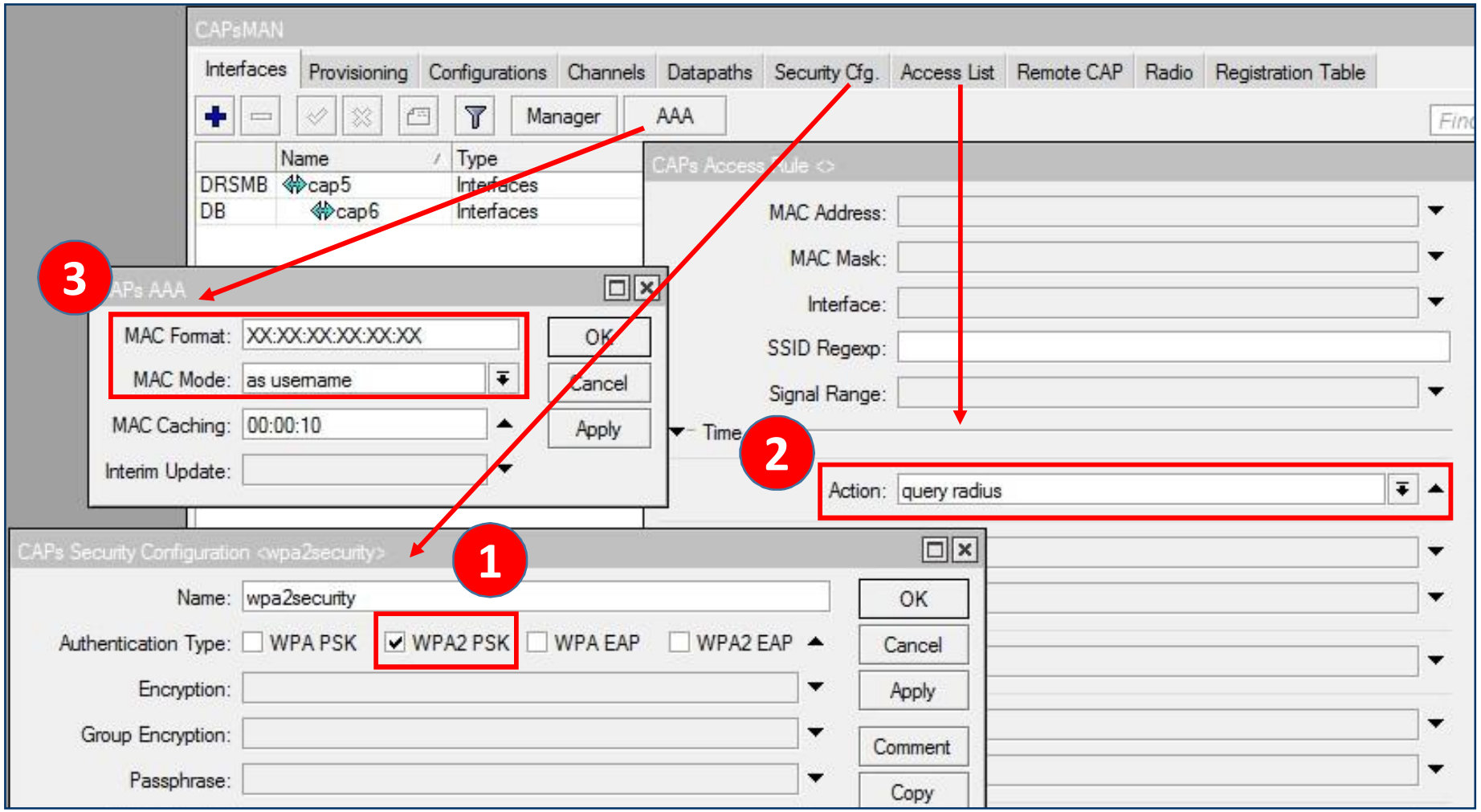
MAC based PSK: Radius

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

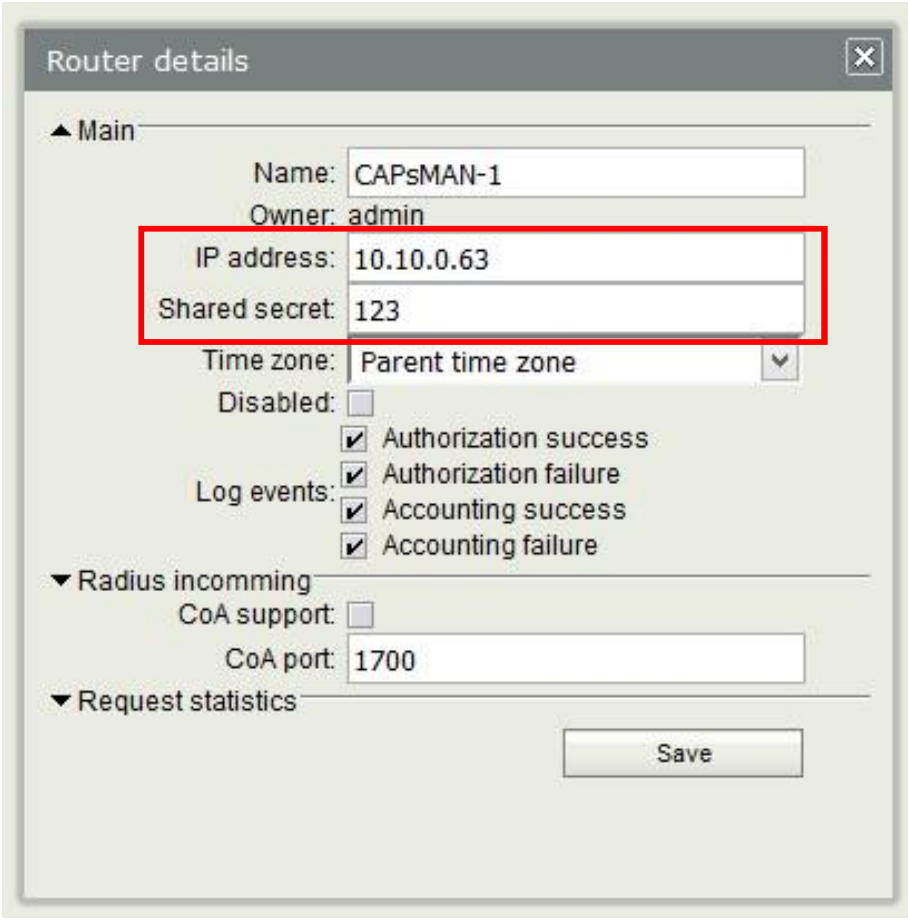


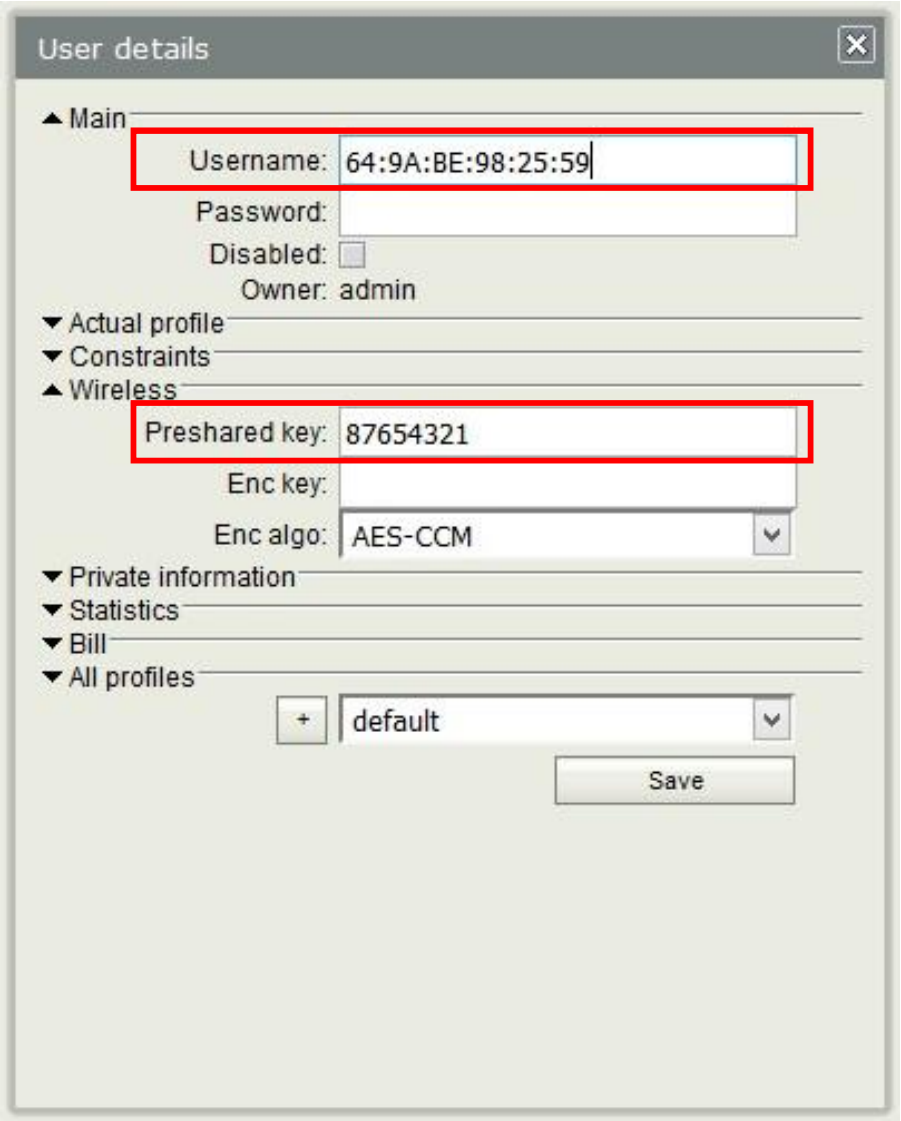


MAC based PSK: CAPsMAN

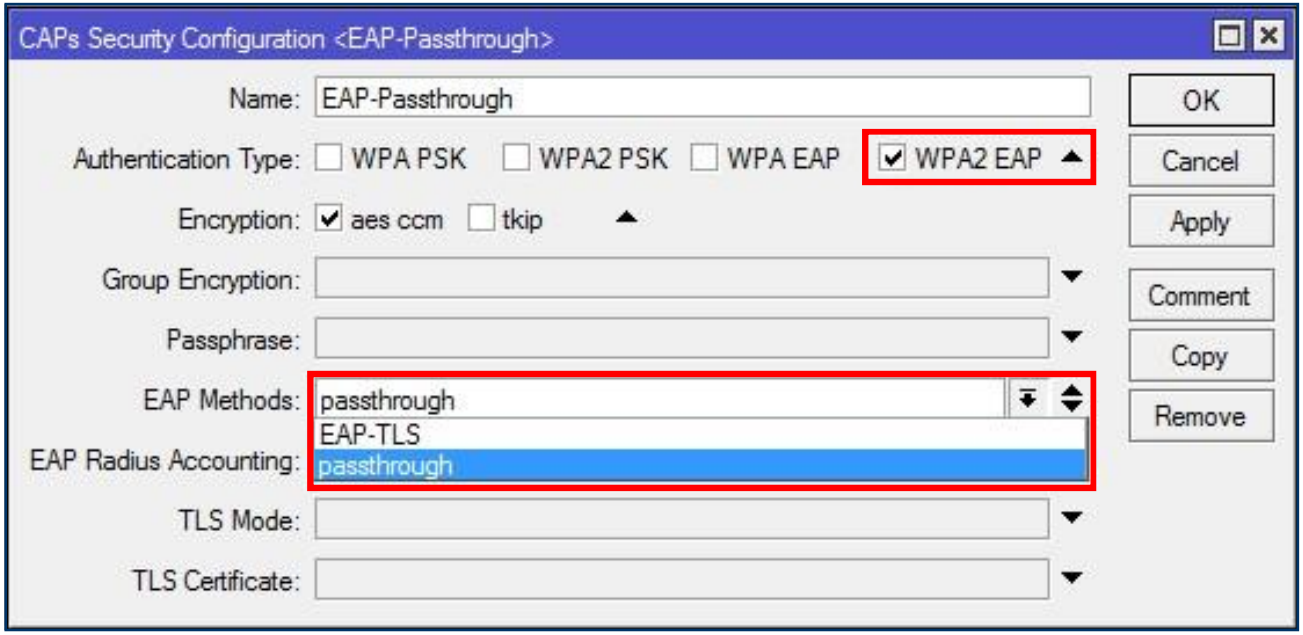


MAC based PSK: Usermanager





WPA-Enterprise



Internally Supported

- EAP-TLS

Externally Supported

- all EAP methods
- passthrough

WPA-Enterprise releated Terms

- 802.1X = 802 AA Standard
- EAP = Extensible Authentication Protocol
- EAP-TLS
- EAP-TTLS
- PEAP (EAP-PEAP) Protected Extensible Authentication Protocol

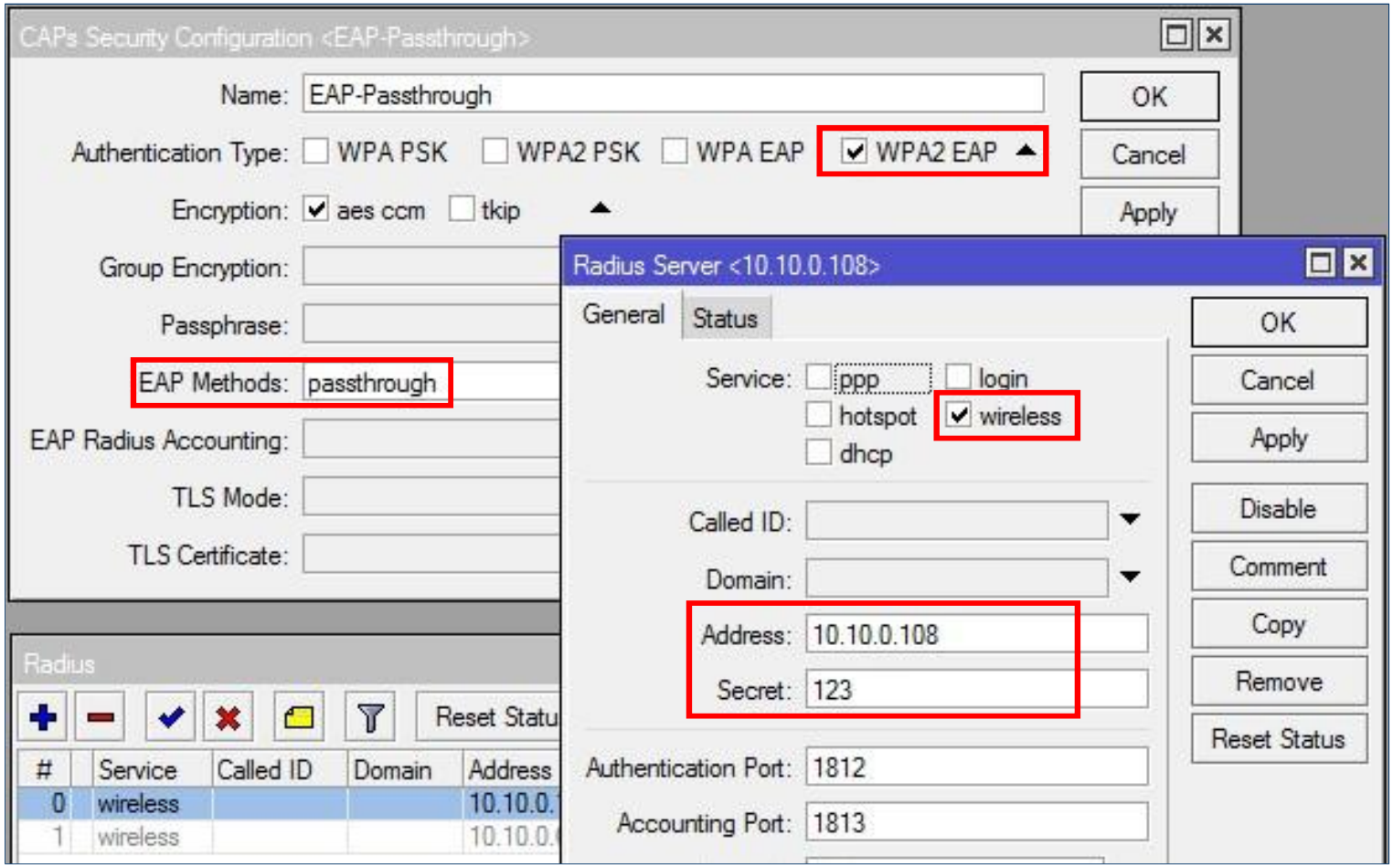
- PEAPv0 with MSCHAPv2 often called PEAP

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



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

ZEROSHELL
Net Services

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

ZEROSHELL
Net Services

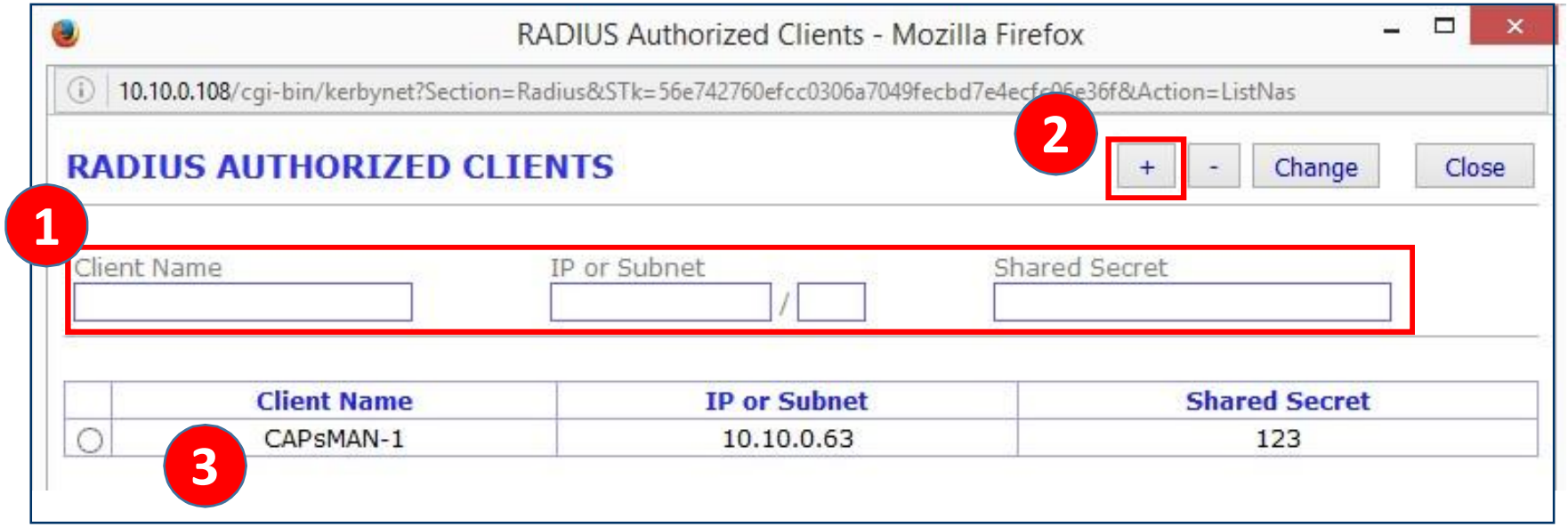
www.zeroshell.org

Zeroshell Configuration

- Enable the Radius Server

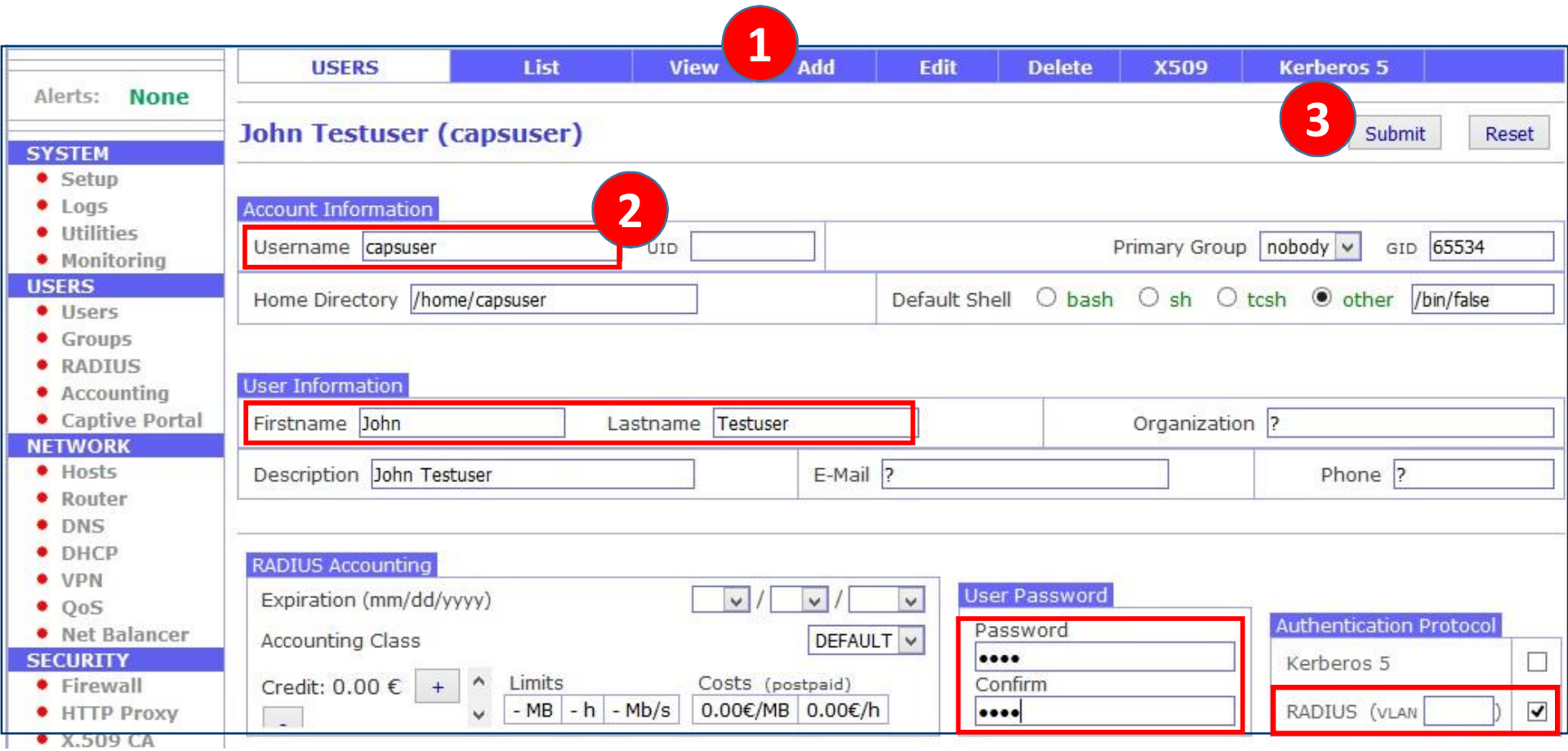
Zeroshell Configuration

- Add an authorised client

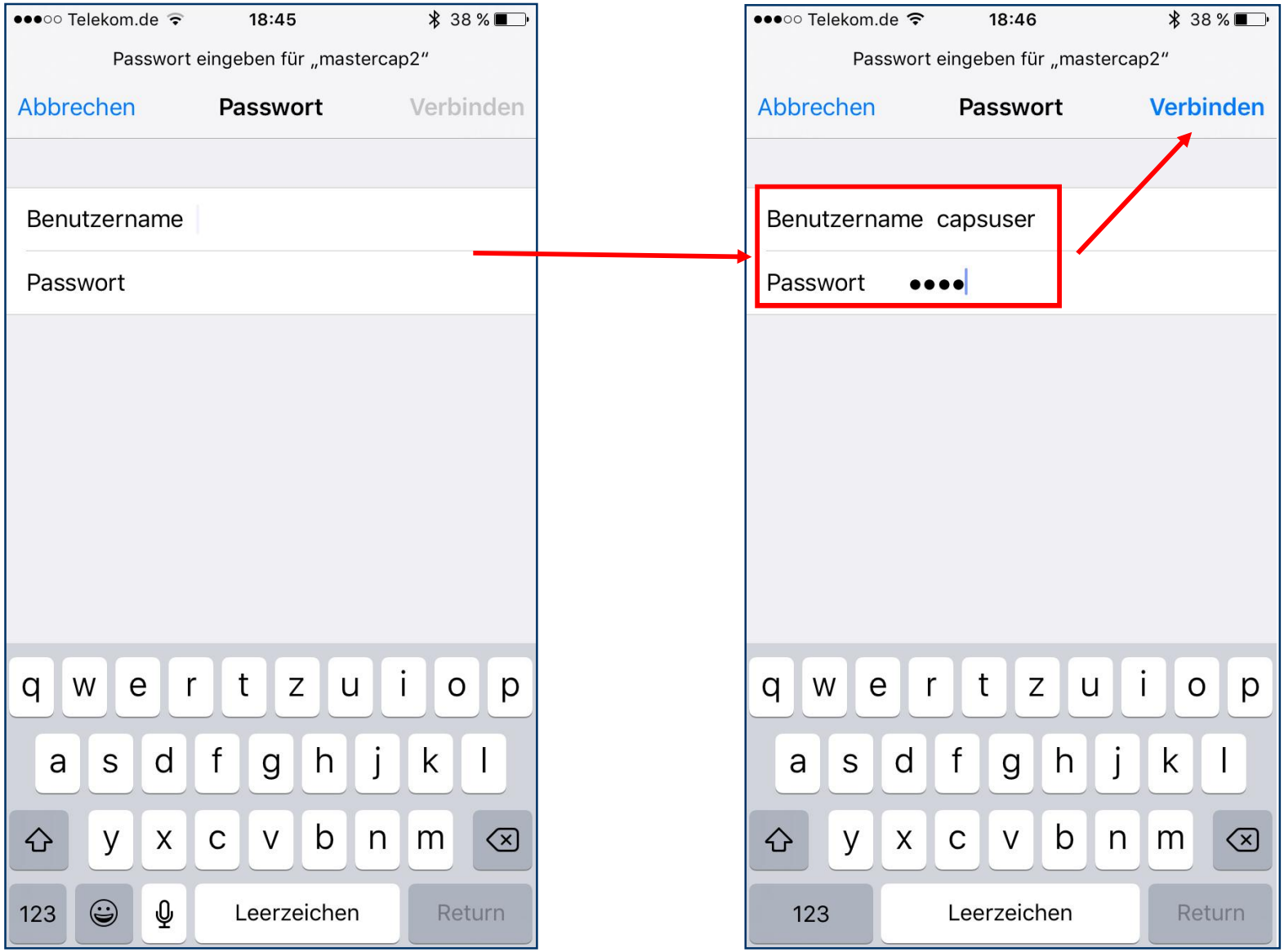


Zeroshell Configuration

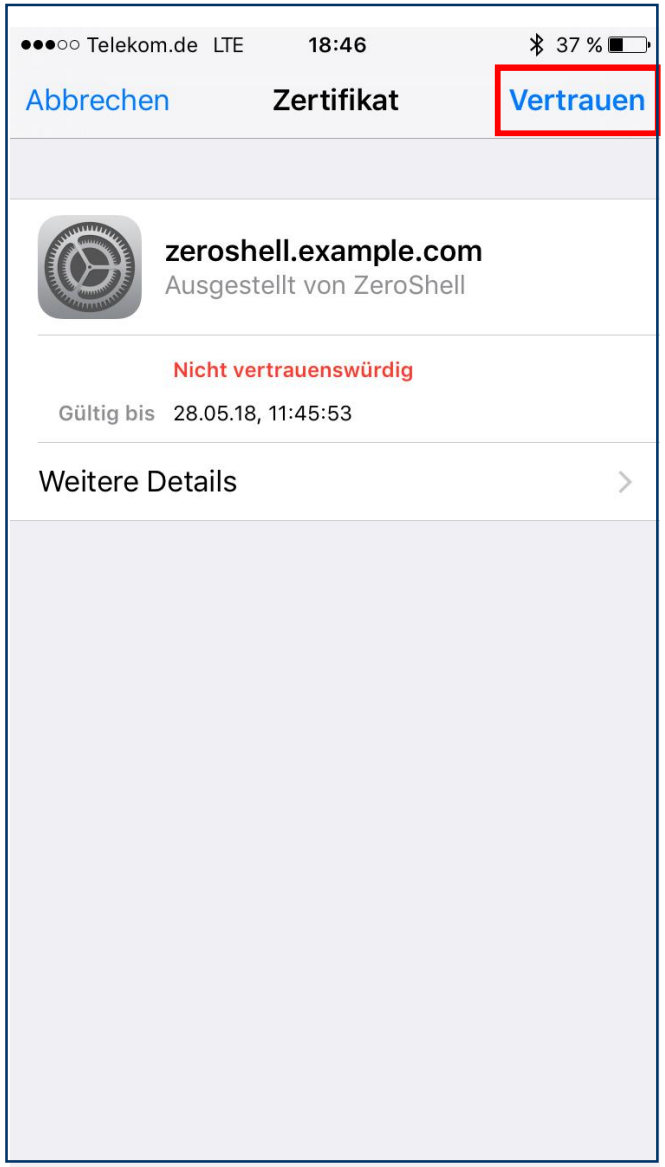
- Add an user account

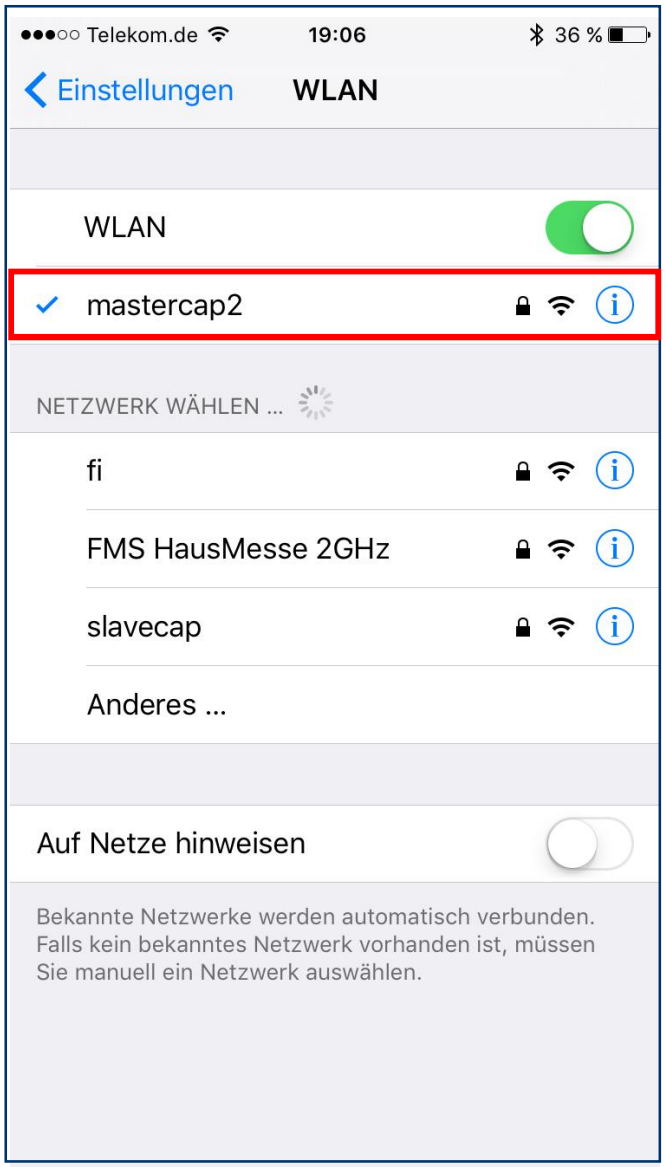


Connect an iPhone with PEAP



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