

# Build enterprise wireless with **CAPsMAN**

Mikrotik User Meeting Yogyakarta,  
October 19-20, 2018

Achmad Mardiansyah

[achmad@glcnetworks.com](mailto:achmad@glcnetworks.com)

GLC Networks, Indonesia

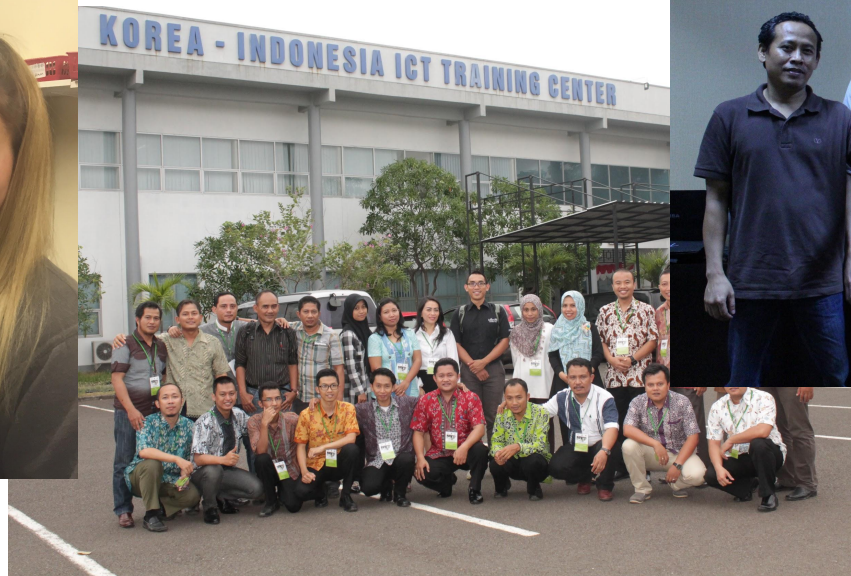
[www.glcnetworks.com](http://www.glcnetworks.com)

# Agenda

- Introduction
- Enterprise wireless
- How CAPsMAN works
- CAPsMAN features
- CAPsMAN tips
- Suggestions for Mikrotik
- Q & A

# What is GLC?

- Garda Lintas Cakrawala ([www.glcnetworks.com](http://www.glcnetworks.com))
- Based in Bandung, Indonesia
- Areas: Training, IT Consulting
- Certified partner for: Mikrotik, Ubiquity, Linux foundation
- Product: GLC radius manager
- Regular event: webinar (every 2 weeks, see our schedule on website)



# About me



- Name: Achmad Mardiansyah
- Base: bandung, Indonesia
- Linux user since 1999, mikrotik user since 2007,
- Mikrotik Certified Trainer  
(MTCNA/RE/WE/UME/INE/TCE/IPv6)
- Mikrotik Certified Consultant
- Teacher at Telkom University (Bandung, Indonesia)
- Website contributor: [achmadjournal.com](http://achmadjournal.com),  
[mikrotik.tips](http://mikrotik.tips), [asysadmin.tips](http://asysadmin.tips)
- More info:  
<http://au.linkedin.com/in/achmadmardiansyah>

# Past experiences



- 2018, **Malaysia**: integrated monitoring system and bandwidth management for a broadband ISP
- 2017, **Libya (north africa)**: remote wireless migration for a new Wireless ISP
- 2016, **United Kingdom**: facilitates workshop for a wireless ISP, migrating a bridged to routed network
- 2015, **West Borneo**: supporting wireless infrastructure project
- 2014, **Senegal (west africa)**: TAC2 engineer for HLR migration from NOKIA to ERICSSON
- 2013, **Malaysia**: build a wireless network to support an international event



# About Telkom University



- Located in Bandung, Indonesia
- 7 Faculties, 27 schools
- Areas: Engineering, Communications, Computing, Business and management, Arts
- 650+ Academic staff, 400+ Administration staff, 20000+ students
- An exchange program
- Runs mikrotik academy program

# Mikrotik academy @ TEL-U

- Started in 2013
- Embedded into schools curriculum
- 100% hands-on
- Get MTCNA certification



# Enterprise wireless



# Characteristics of enterprise wireless

- Usually indoor, on access network (directly connected to end-user)
- PTMP (point to multi point)
- **Centralised** FCAPS (Fault, Configuration, Authentication, Performance, Security)
- **Enterprise features:** load balancing, better mobility (seamless roaming), security, high availability, authentication, band steering, security
- Example: office, campus, hotel

# How CAPsMAN works

# About CAPsMAN

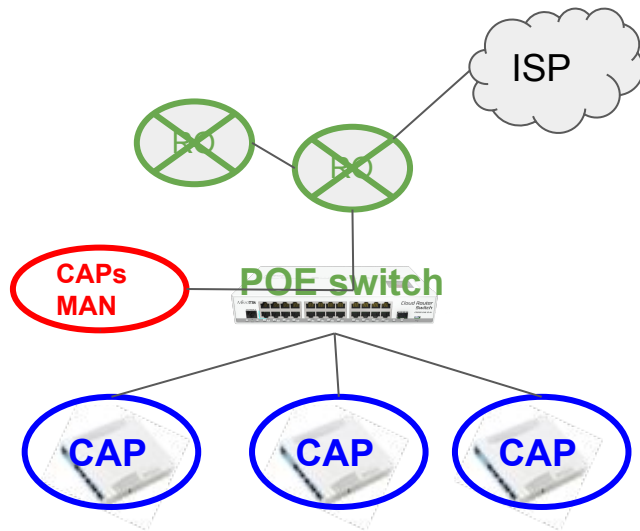
- Offers enterprise features: centralised platform to manage AP
- Software based, free to use
- Available since 6.11, CAPsMAN v1 (march 2014)
- Now its CAPsMAN v2 (since 6.22, nov 2014). Recommended version, not compatible to v1
- CAP: controlled AP
- CAPsMAN: CAP manager (AP controller)



# CAPsMAN - CAP connectivity

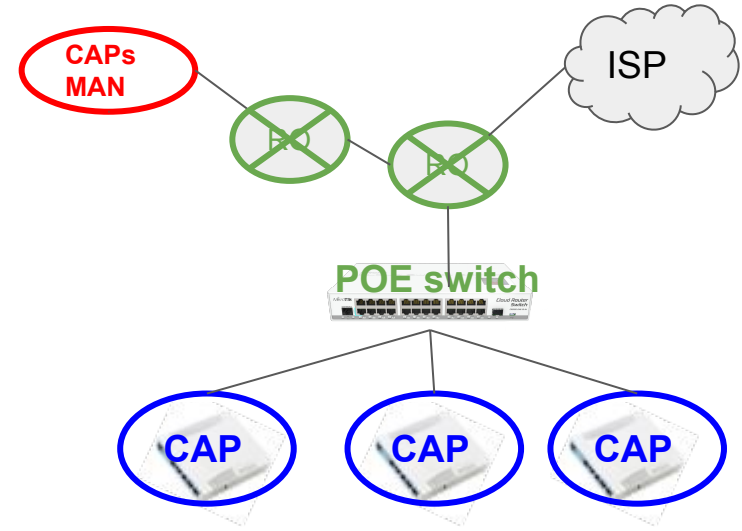
## Layer 2

- CAP and CAPsMAN are in the same network

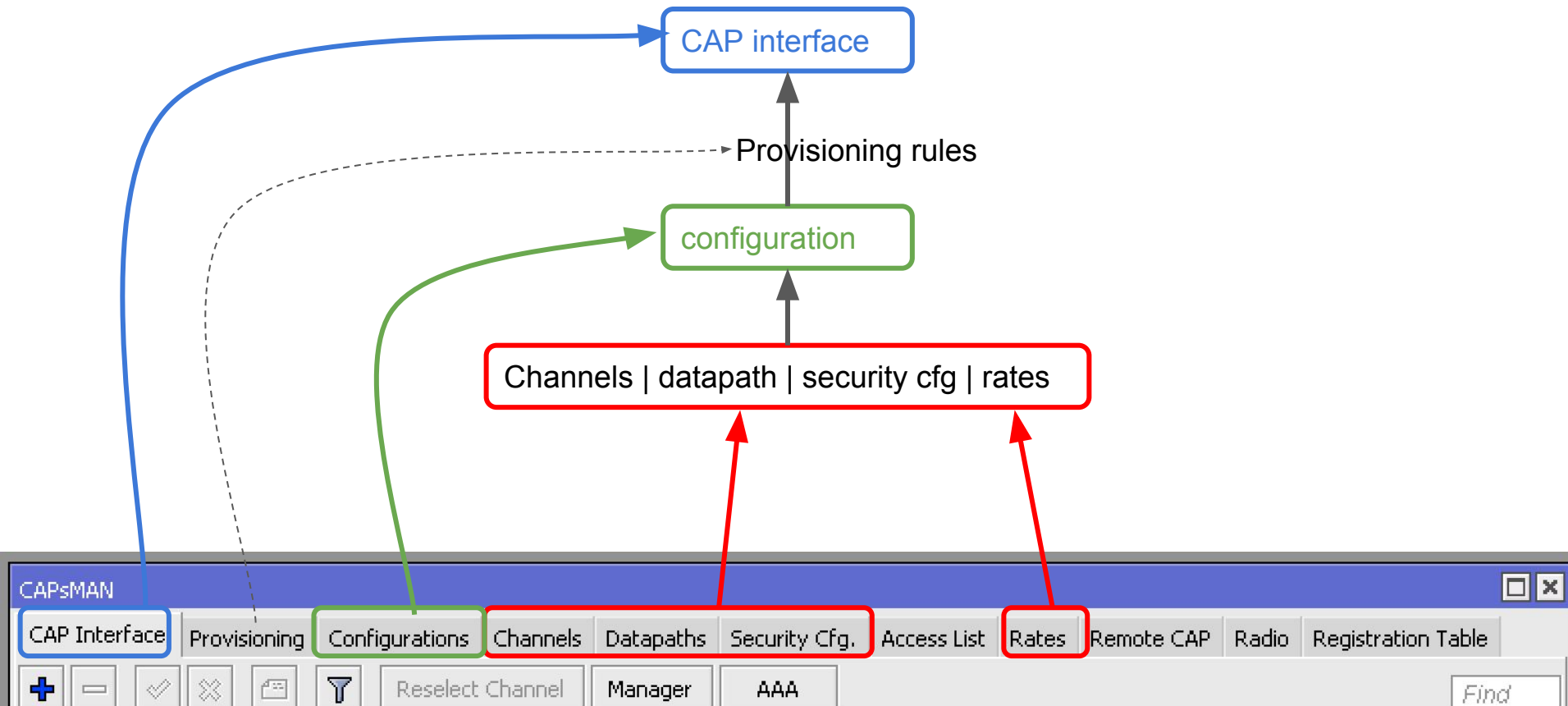


## Layer 3 (recomm.)

- CAP and CAPsMAN are in different network



# CAPsMAN configuration concepts



# Channels | datapath | security cfg | rates

CAP Interface Provisioning Configurations **Channels** Datapaths Security Cfg

+ - [icon] [icon]

Name	Frequency	Control C...	Band	Extension Ch...	Tx Power
F-2412	2412	20Mhz	2ghz-g/n	disabled	17
F-2437	2437	20Mhz	2ghz-g/n	disabled	17
F-2462	2462	20Mhz	2ghz-g/n	disabled	17
F-5745	5745	20Mhz	5ghz-a/n/ac	disabled	17

CAP Interface Provisioning Configurations Channels **Datapaths** Security Cfg. Access L

+ - [icon] [icon]

Name	Bridge	Open...	Local Forw...	Client To Cl...	VLAN Mode	VLAN ID
dp-lf			yes	no		
;;; vlan 22						
dp-lf-vlan22			yes	no	use service tag	22

CAP Interface Provisioning Configurations Channels Datapaths **Security Cfg.** Access List Rate

+ - [icon] [icon]

Name	Authentication T...	Encryption	Group Enc...	Group Key...	Passphrase
wpa-psk-ddsatuvisi	WPA PSK WPA2 ...	aes ccm	aes ccm		*****
wpa-psk-old	WPA PSK WPA2 ...	aes ccm	aes ccm		*****

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

+ - [icon] [icon]

Name	Basic Rates	Supported Rates	HT Basic MCS	HT Supported MCS	VHT Basic MCS	VHT Supported MCS
rate-default		9Mbps 12Mbps 18Mb...		3 4 5 6 7 11 12 13 14...	none	MCS 0-9, MCS 0-...

# configuration

New CAPs Configuration

Wireless Channel Rates Datapath Security

Name:

Mode:

SSID:

Hide SSID:

Load Balancing Group:

Distance:  km

Hw. Retries:

Hw. Protection Mode:

Frame Lifetime:

Disconnect Timeout:

Keepalive Frames:

Country:

Max Station Count:

Multicast Helper:

HT Tx Chains:  0  1  2

HT Rx Chains:  0  1  2

HT Guard Interval:

wireless Channel Rates Datapath Security

Rate:

- Basic Rates
- Supported Rates
- HT Basic MCS
- HT Supported MCS
- VHT Basic MCS
- VHT Supported MCS

Wireless Channel Rates Datapath Security

Channel:

Frequency:

Control Channel Width:

Band:

Extension Channel:

Tx Power:

Save Selected:

Reselect Interval:

Skip DFS Channels:

Wireless Channel Rates Datapath Security

Security:

Authentication Type:

Encryption:

Group Encryption:

Group Key Update:

Passphrase:

EAP Methods:

EAP Radius Accounting:

TLS Mode:

TLS Certificate:

Wireless Channel Rates Datapath Security

Datapath:

MTU:

L2 MTU:

ARP:

Bridge:

Bridge Cost:

Bridge Horizon:

OpenFlow Switch:

Local Forwarding:

Client To Client Forwarding:

VLAN Mode:

VLAN ID:

Interface List:

# Provisioning rule

CAPsMAN

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

+ - ✓ ✗ 📁 🔍 Find

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

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

Hw. Supported Modes: g  
gn

Identity Regexp: GP-AP-1.3

Common Name Regexp:

IP Address Ranges: 10.10.24.2-10.10.31.254

Action: create enabled

Master Configuration: master1-2ghz

Slave Configuration: DDF  
DDF\_FASTER

Name Format: identity

Name Prefix:

enabled

OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove

New CAPs Provisioning

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

Hw. Supported Modes: ac

Identity Regexp: GP-AP-1.3

Common Name Regexp:

IP Address Ranges: 10.10.24.2-10.10.31.254

Action: create enabled

Master Configuration: master1-5ghz

Slave Configuration: DDF  
DDF\_FASTER

Name Format: identity

Name Prefix:

enabled

OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove

16

NETWORKS University



# Master vs slave configuration

## Master

- Will be used to set basic wireless parameters: Frequency, channel-width, TX power

## Slave

- Basic wireless parameter will be ignored
- Is used to setup additional SSID (Virtual AP)

# CAP interface

The screenshot displays a network management interface for configuring CAP (Client Access Point) interfaces. The left pane shows a list of interfaces, with GP-AP-1.1-1 highlighted as the 'master interface' and other GP-AP interfaces listed as 'Slave interface'. The right pane shows the configuration for the selected interface, GP-AP-1.1-1.

**Master Interface:** GP-AP-1.1-1

**Slave Interfaces:** GP-AP-1.1-1-1, GP-AP-1.1-1-2, GP-AP-1.1-2, GP-AP-1.1-2-1, GP-AP-1.2-1-1, GP-AP-1.2-1-2, GP-AP-1.2-2, GP-AP-1.2-2-1, GP-AP-1.2-2-2, GP-AP-1.3-1, GP-AP-1.3-2, GP-AP-2.1-1, GP-AP-2.1-1-1, GP-AP-2.1-1-2

**Interface <GP-AP-1.1-1> Configuration:**

- Last Link Down Time: May/17/2018 20:21:02
- Last Link Up Time: May/17/2018 16:00:51
- Link Downs: 5
- Current State: running-ap
- Current Channel: 2412/20(gn(17dBm))
- Current Rate Set: OFDM:9-54 BW:1x SGI:1x HT:3-7,11-15
- Current Basic Rate Set:
- Current Registered Clients: 0
- Current Authorized Clients: 0

# CAPsMAN features

# Access list

- Is used to control wifi access
- Format:
  - Client matching
  - Action:
    - accept | reject | query radius
  - Connection parameter

## Notes:

- **Client tx limit** is for mikrotik devices only

CAPs Access Rule <>

MAC Address:

MAC Mask:

Interface: all

SSID Regexp:

Signal Range: -80..-10

Allow Signal Out Of Range: 00:00:10

Time

Action: accept

AP Tx Limit:

Client Tx Limit:

Private Passphrase:

Client To Client Forwarding:

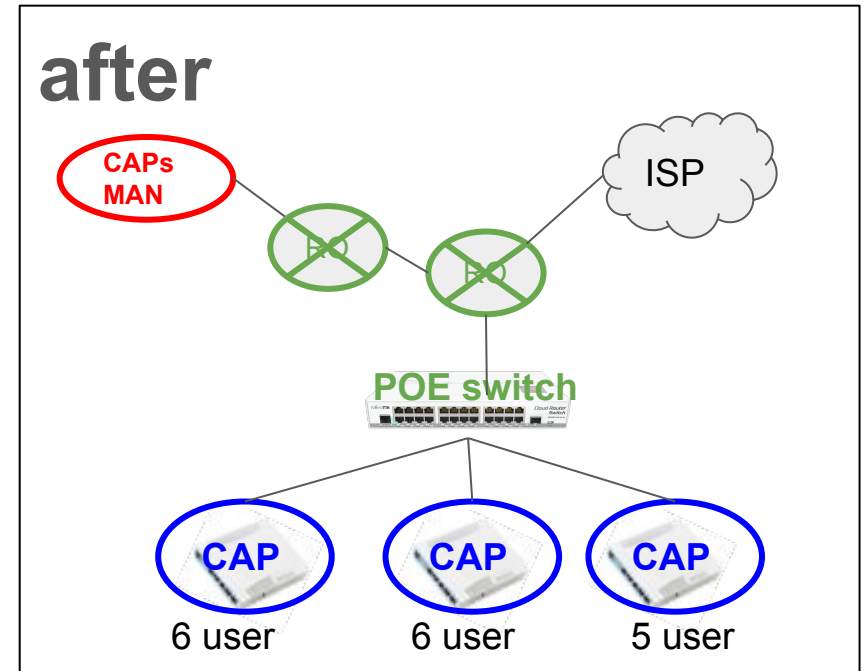
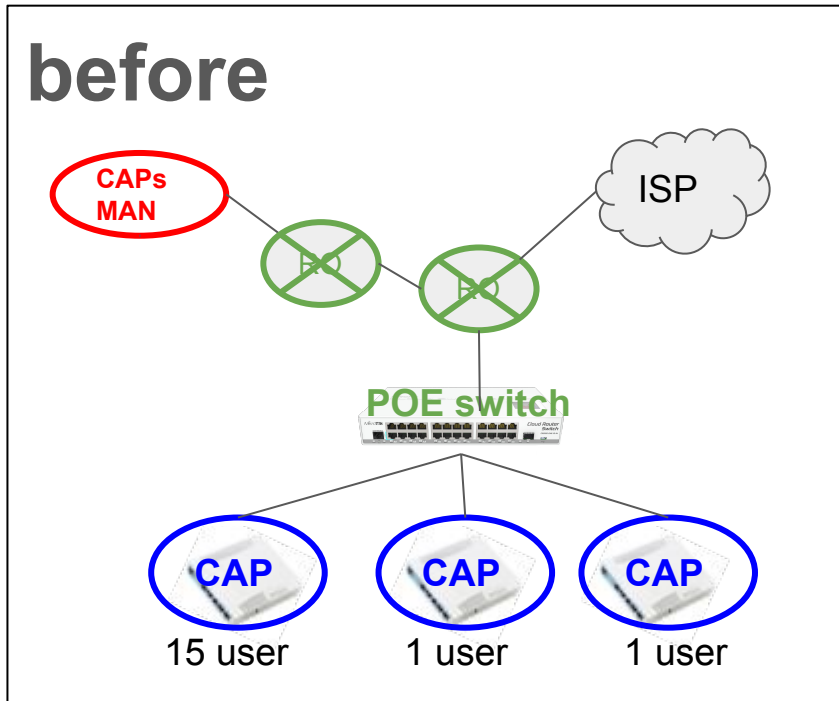
RADIUS Accounting:

VLAN Mode:

VLAN ID:

enabled

# Load balancing AP



Name:

Mode:  ▼ ▲

SSID:  ▲

Hide SSID:  ▼

Load Balancing Group:  ▼ ▲

# Roaming

- Unlike GSM, connection to AP is end-user decision, not AP.
- Often, station is **still attached to old AP** even though already moved to new AP
- What AP can set up a threshold for disassociation (based on signal level)
- On CAPsMAN, we use **access rule**

CAPs Access Rule <>

MAC Address:

MAC Mask:

Interface: all

SSID Regexp:

Signal Range: -80..-10

Allow Signal Out Of Range: 00:00:10

Time

Action: accept

CAPs Access Rule <>

MAC Address:

MAC Mask:

Interface: all

SSID Regexp:

Signal Range: -120..-81

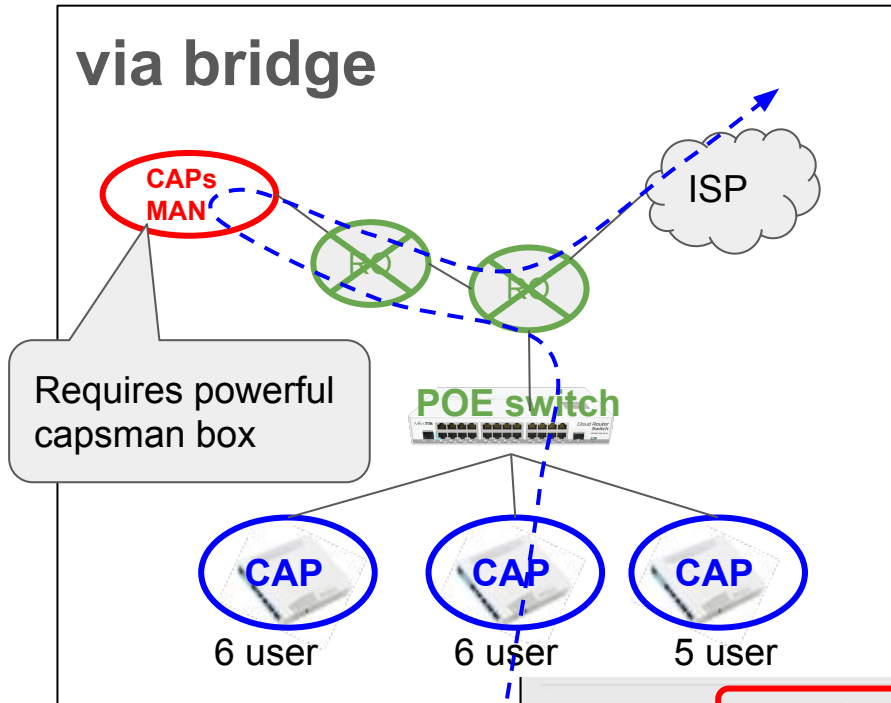
Allow Signal Out Of Range: 00:00:10

Time

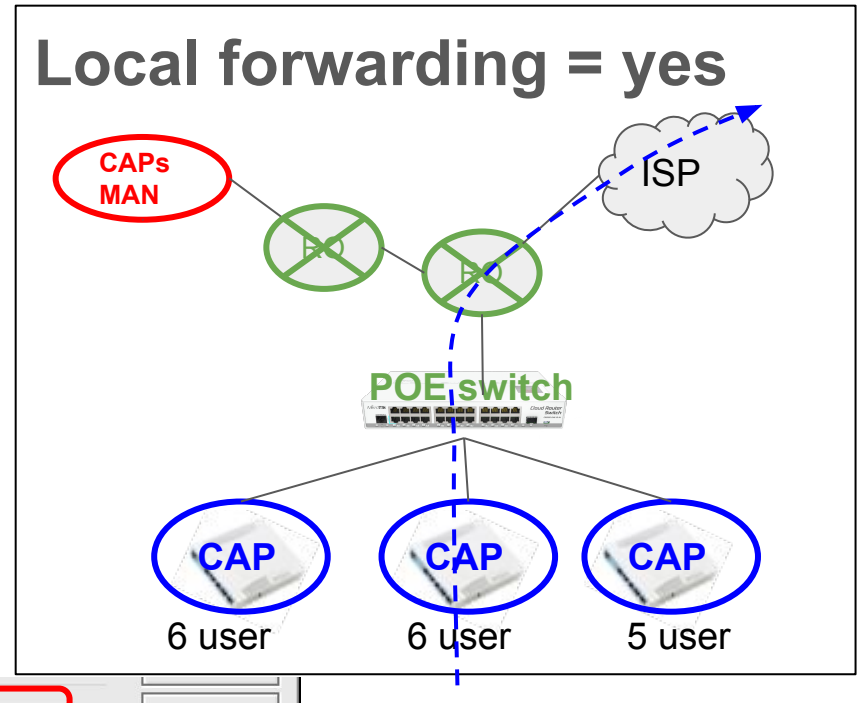
Action: reject

# Datapath (local forwarding)

via bridge



Local forwarding = yes



Bridge:  Copy

Bridge Cost:  Remove

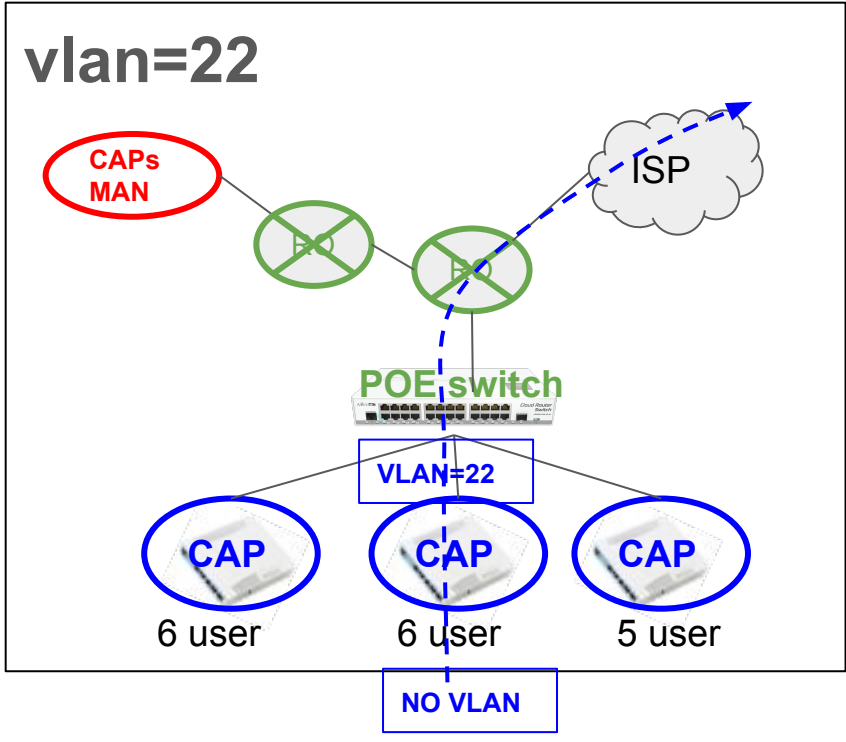
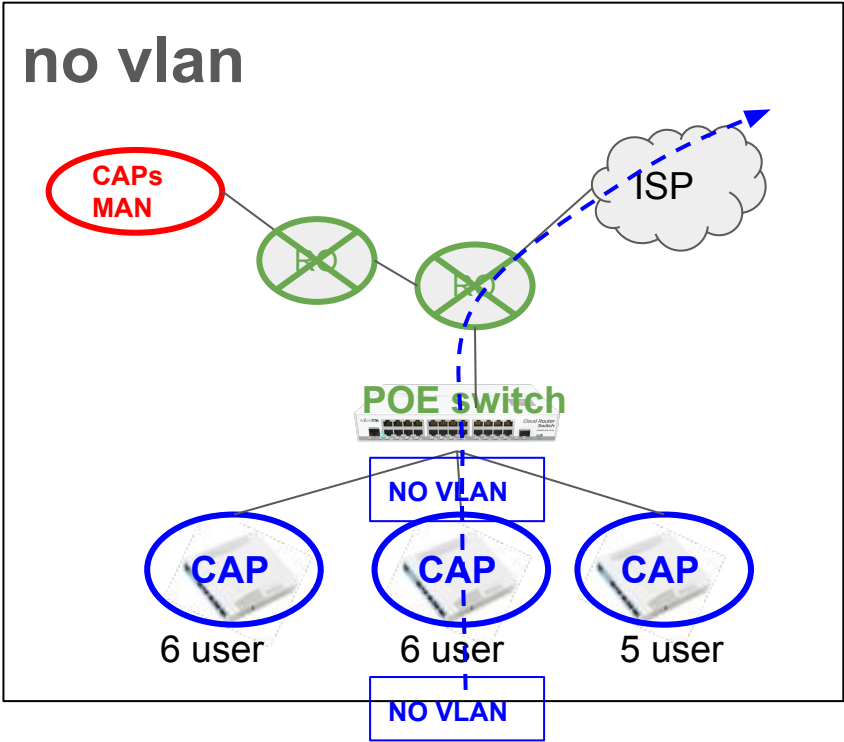
Bridge Horizon:

OpenFlow Switch:

Local Forwarding:

Client To Client Forwarding:

# Datapath (vlan)



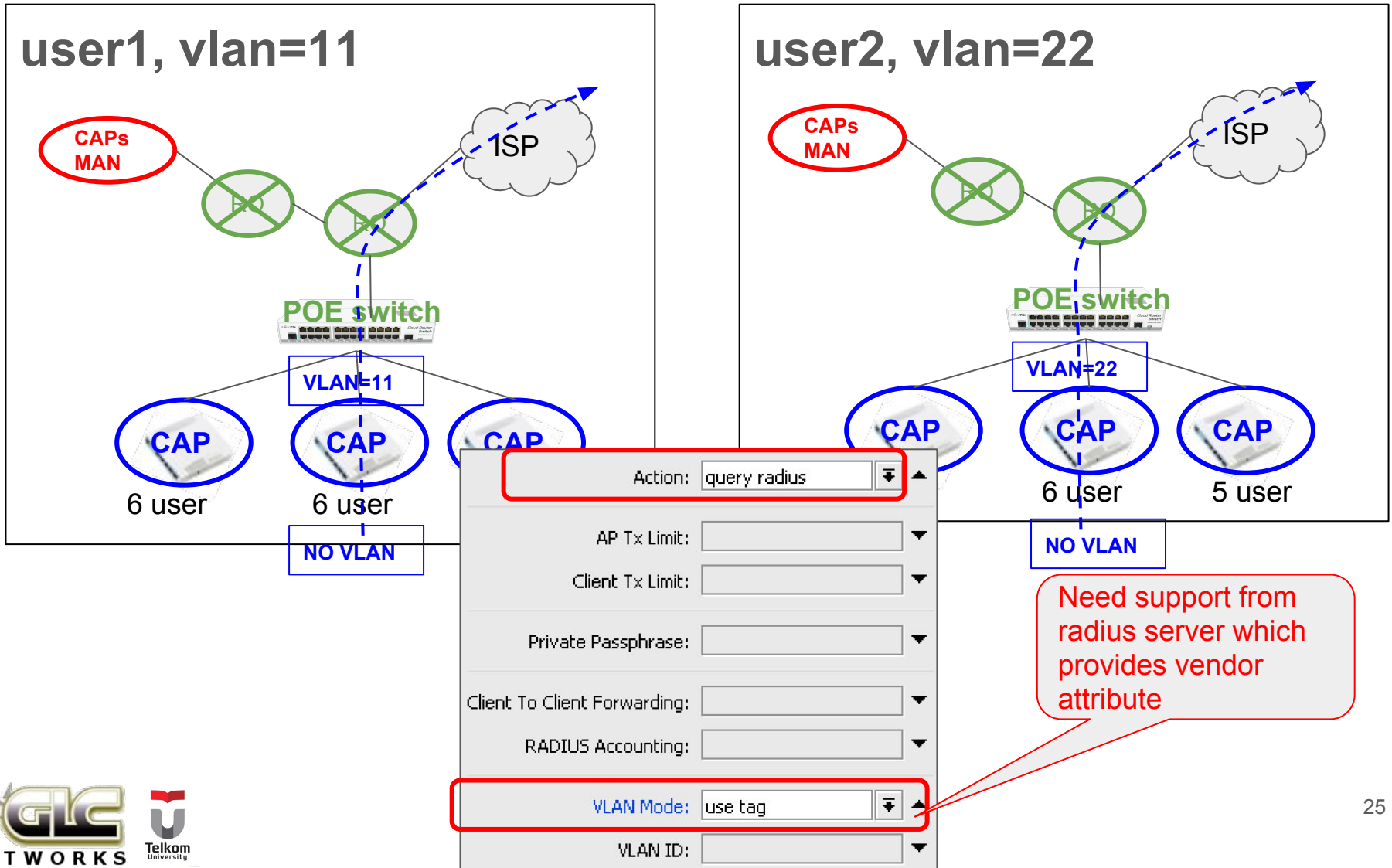
VLAN Mode: use tag

VLAN ID: 22

Interface List:

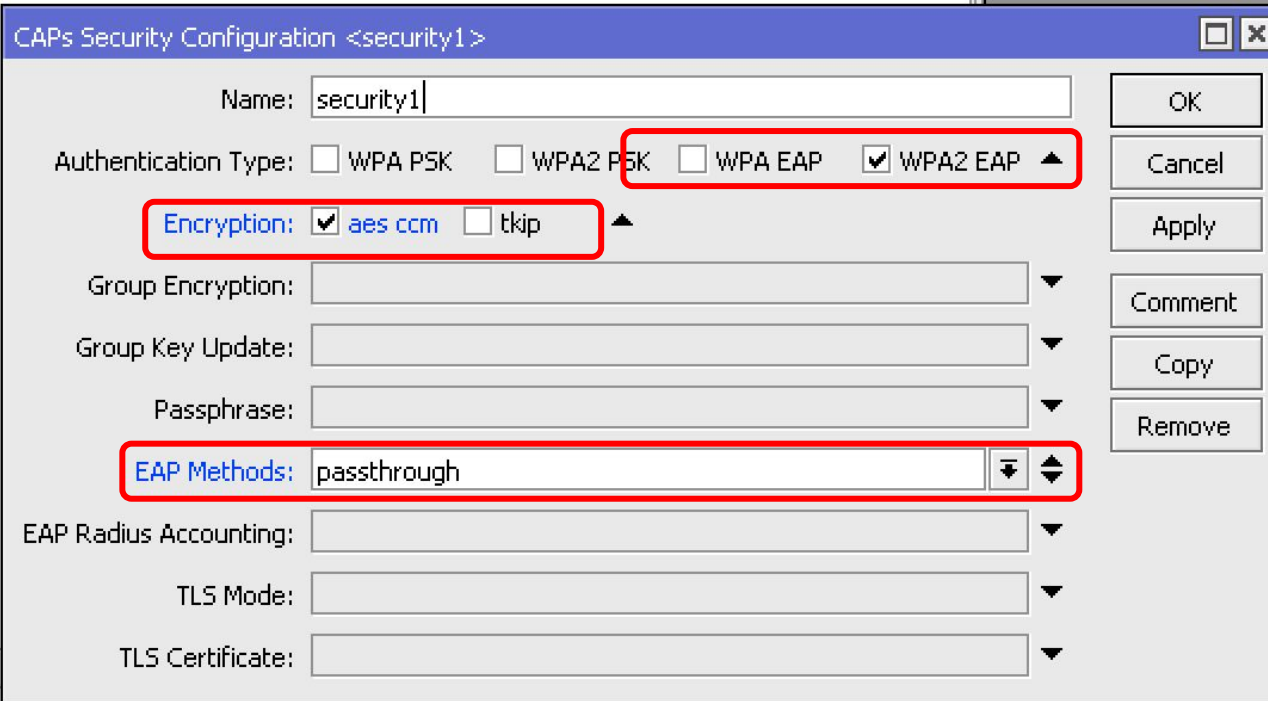


# Datapath (vlan per user)



# Security: EAP (layer 2 authentication)

- Username and password will be asked on layer2
- Need support from radius server



The screenshot shows a configuration window titled "CAPs Security Configuration <security1>". The "Name" field contains "security1". Under "Authentication Type", the "WPA2 EAP" option is selected with a checkmark. The "Encryption" section shows "aes ccm" selected with a checkmark, while "tkip" is unselected. The "EAP Methods" dropdown menu is set to "passthrough". Other fields like "Group Encryption", "Group Key Update", "Passphrase", "EAP Radius Accounting", "TLS Mode", and "TLS Certificate" are empty. On the right side, there are buttons for "OK", "Cancel", "Apply", "Comment", "Copy", and "Remove".

# MAC based authentication

- It is possible to allow client to connect based on MAC address
- We need support from radius server which contains MAC address database
- Combined with access-list

CAPs Access Rule <>

MAC Address:

MAC Mask:

Interface: all

SSID Regexp: OneVision.\*

Signal Range: -80..-10

Allow Signal Out Of Range: 00:00:10

Time

Action: query radius

AP Tx Limit:

Client Tx Limit:

Private Passphrase:

Client To Client Forwarding:

RADIUS Accounting:

VLAN Mode:

VLAN ID:

enabled

# CAPsMAN tips

# CAP: use auto certificate

- Use certificate for **stable** CAP - CAPsMAN connection
- Use “Lock to CAPsMAN” to bind CAP to a particular CAPsMAN

The screenshot displays the configuration page for a CAP (Client Authentication Protocol) in a network management system. The page is titled "CAP" and contains several configuration fields:

- Enabled:** A checkbox that is checked, indicating the CAP is active.
- Interfaces:** Two dropdown menus showing "wlan1" and "wlan2".
- Certificate:** A dropdown menu showing "request", which is highlighted with a red box.
- Discovery Interfaces:** A dropdown menu showing "wlan1".
- Lock To CAPsMAN:** A checkbox that is checked, also highlighted with a red box.
- CAPsMAN Addresses:** Two text input fields containing "10.10.21.60" and "10.10.21.1".
- CAPsMAN Names:** An empty text input field.
- CAPsMAN Certificate Common Names:** An empty text input field.
- Bridge:** A dropdown menu showing "bridge-local".
- Static Virtual:** A checkbox that is checked.
- Requested Certificate:** A text input field containing "CAP-CC2DE02B53BD".
- Locked CAPsMAN Common Name:** A text input field containing "CAPsMAN-A24894AB8D3D".

# CAP: high availability

- If no connection between CAP and CAPsMAN, **station will be disconnected**
- Use more than 1 CAPsMAN for high availability

The screenshot shows the configuration page for a CAP (Client Access Point) in a network management system. The page is titled "CAP" and contains several configuration fields. A red box highlights the "CAPsMAN Addresses" field, which is set to "10.10.21.60" and "10.10.21.1". Other fields include "Enabled" (checked), "Interfaces" (wlan1, wlan2), "Certificate" (request), "Discovery Interfaces" (wlan1), "Lock To CAPsMAN" (checked), "CAPsMAN Names", "CAPsMAN Certificate Common Names", "Bridge" (bridge-local), "Static Virtual" (checked), "Requested Certificate" (CAP-CC2DE02B53BD), and "Locked CAPsMAN Common Name" (CAPsMAN-A24894AB8D3D).

Enabled	<input checked="" type="checkbox"/>
Interfaces:	wlan1
	wlan2
Certificate:	request
Discovery Interfaces:	wlan1
Lock To CAPsMAN	<input checked="" type="checkbox"/>
CAPsMAN Addresses:	10.10.21.60
	10.10.21.1
CAPsMAN Names:	
CAPsMAN Certificate Common Names:	
Bridge:	bridge-local
Static Virtual	<input checked="" type="checkbox"/>
Requested Certificate:	CAP-CC2DE02B53BD
Locked CAPsMAN Common Name:	CAPsMAN-A24894AB8D3D

# CAPsMAN: upgrade CAP version

- It is recommended to use latest version of RouterOS
- CAPsMAN can upgrade CAP
- CAPs do not need to connect to internet directly

CAPs Manager

Enabled

Certificate:

CA Certificate: auto

Require Peer Certificate

Generated Certificate:

Generated CA Certificate: CAPsMAN-CA-694D850...

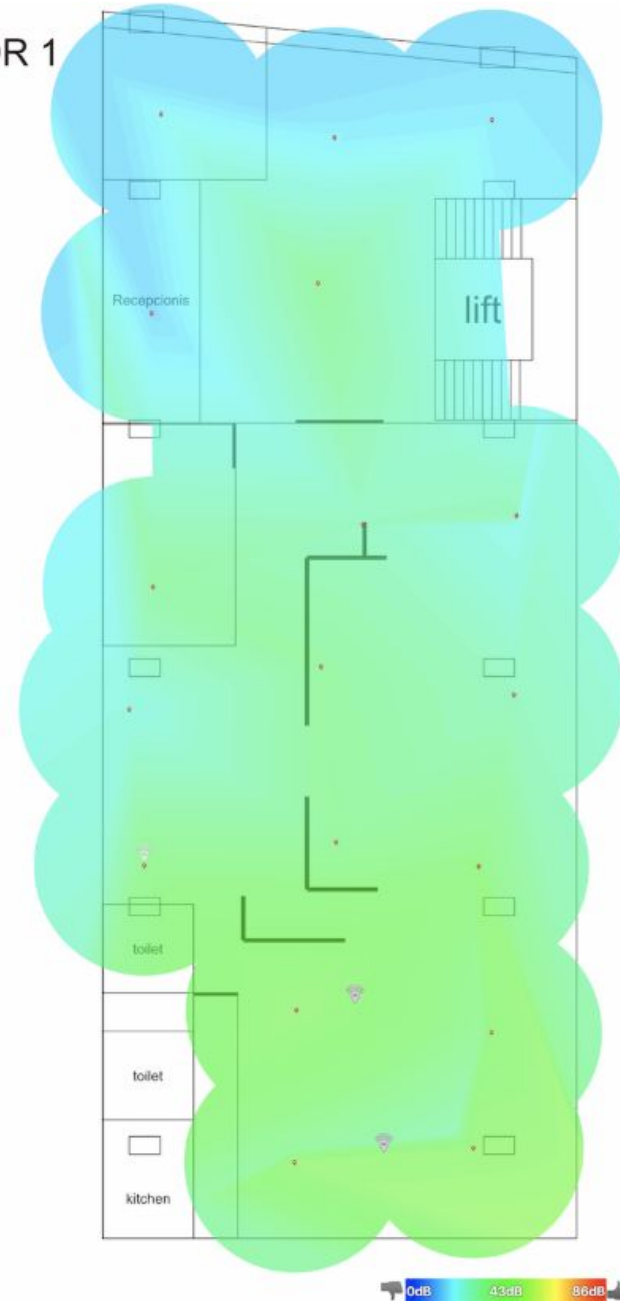
Package Path: /capsman

Upgrade Policy: suggest same version

# Wireless survey

- Wireless survey is very useful for troubleshooting and verify your wireless setting

FLOOR 1  
1:100





# Enable client isolation and port isolation

- To gain more airtime, better if we disable client-to-client communication:
  - Do not activate “client-to-client forwarding”
  - Apply port isolation. Check your switch documentation
  - Do not put server on wireless network. Example: wireless printer

CAPs Datapath Configuration <dp-lf >

Name:

MTU:  ▼

L2 MTU:  ▼

ARP:  ▼

---

Bridge:  ▼

Bridge Cost:  ▼

Bridge Horizon:  ▼

---

OpenFlow Switch:  ▼

---

Local Forwarding:  ▲

Client To Client Forwarding:  ▲

---

VLAN Mode:  ▼

VLAN ID:  ▼

Interface List:  ▼

# Smooth mobility for client

- Maintain layer 3 address. Changing on layer 3 address (ex. renew dhcp-client ip address) will make disconnection time longer.
- Can use flat layer 3 network for whole wireless. Check layer 2 vendor to minimise broadcast traffic
- Can use vlan id per user

FLOOR 1  
1:100



# Flexible provisioning

- Setup pattern on CAP identity
- Use regex facility on CAPsMAN provisioning

New CAPs Provisioning

Radio MAC:

Hw. Supported Modes:

**Identity Regexp:**

Common Name Regexp:

IP Address Ranges:

Action:

Master Configuration:

Slave Configuration:

Name Format:

Name Prefix:

# Flexible provisioning

- Setup pattern on CAP identity
- Use regex facility on CAPsMAN provisioning

New CAPs Provisioning

Radio MAC:

Hw. Supported Modes:

**Identity Regexp:**

Common Name Regexp:

IP Address Ranges:

Action:

Master Configuration:

Slave Configuration:

Name Format:

Name Prefix:

# VLAN ID per user

- Meaning, we dont need to provide different SSID for group of users.  
E.g. ssid for teacher, ssid for students
- Need support from radius

New CAPs Datapath Configuration

Name: datapath1

MTU: [ ]

L2 MTU: [ ]

ARP: [ ]

Bridge: bridge-local

Bridge Cost: [ ]

Bridge Horizon: [ ]

OpenFlow Switch: [ ]

Local Forwarding: [ ]

Client To Client Forwarding: [ ]

VLAN Mode: use tag

VLAN ID: [ ]

Interface List: [ ]

OK  
Cancel  
Apply  
Comment  
Copy  
Remove

ATTRIBUTE	Mikrotik-Wireless-Forward	4	integer
ATTRIBUTE	Mikrotik-Wireless-Skip-Dot1x	5	integer
ATTRIBUTE	Mikrotik-Wireless-Enc-Algo	6	integer
ATTRIBUTE	Mikrotik-Wireless-Enc-Key	7	string
ATTRIBUTE	Mikrotik-Rate-Limit	8	string
ATTRIBUTE	Mikrotik-Realm	9	string
ATTRIBUTE	Mikrotik-Host-IP	10	ipaddr
ATTRIBUTE	Mikrotik-Mark-Id	11	string
ATTRIBUTE	Mikrotik-Advertise-URL	12	string
ATTRIBUTE	Mikrotik-Advertise-Interval	13	integer
ATTRIBUTE	Mikrotik-Recv-Limit-Gigawords	14	integer
ATTRIBUTE	Mikrotik-Xmit-Limit-Gigawords	15	integer
ATTRIBUTE	Mikrotik-Wireless-PSK	16	string
ATTRIBUTE	Mikrotik-Total-Limit	17	integer
ATTRIBUTE	Mikrotik-Total-Limit-Gigawords	18	integer
ATTRIBUTE	Mikrotik-Address-List	19	string
ATTRIBUTE	Mikrotik-Wireless-MPKey	20	string
ATTRIBUTE	Mikrotik-Wireless-Comment	21	string
ATTRIBUTE	Mikrotik-Delegated-IPv6-Pool	22	string
ATTRIBUTE	Mikrotik_DHCP_Option_Set	23	string
ATTRIBUTE	Mikrotik_DHCP_Option_Param_STR1	24	string
ATTRIBUTE	Mikrotik_DHCP_Option_Param_STR2	25	string
ATTRIBUTE	Mikrotik_Wireless_VLANID	26	integer
ATTRIBUTE	Mikrotik_Wireless_VLANIDtype	27	integer
ATTRIBUTE	Mikrotik_Wireless_Minsignal	28	string
ATTRIBUTE	Mikrotik_Wireless_Maxsignal	29	string

# Suggestions for mikrotik

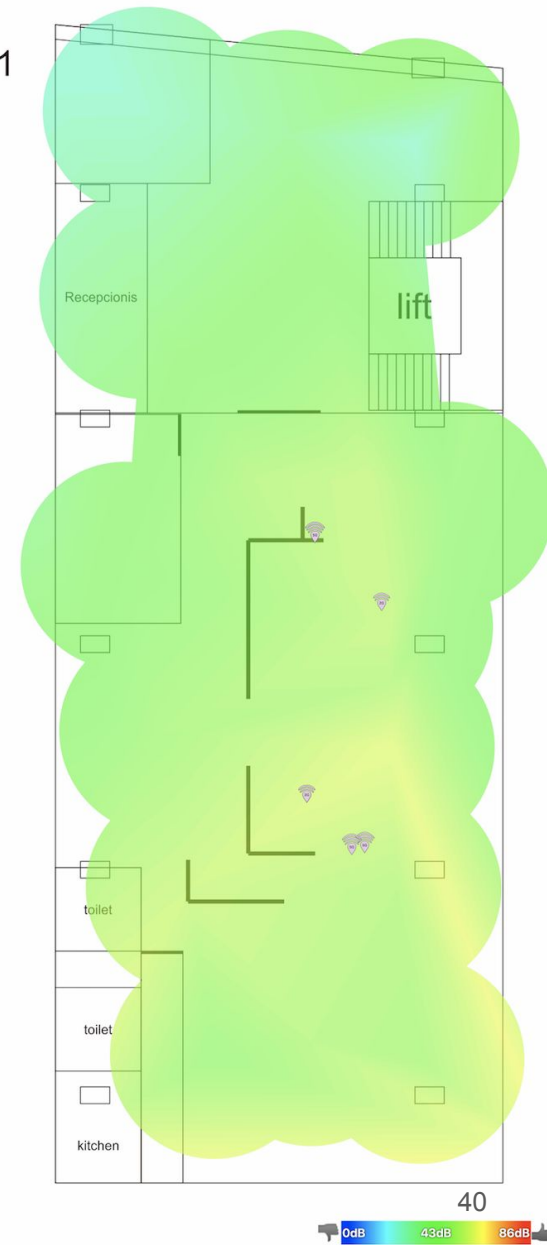
# Automatic band steering

- We encourage users to connect to 5GHz band as it's less crowded compared to 2GHz band
- Currently it's done manually. Example:
  - 2GHz, SSID = wifi
  - 5GHz, SSID = wifi\_faster
- In the future, this process needs to be automatic

# Signal visualisation on floor layout

- Similar to wifi survey
- Useful to check wireless settings
- Thedude integration?

FLOOR 1  
1:100

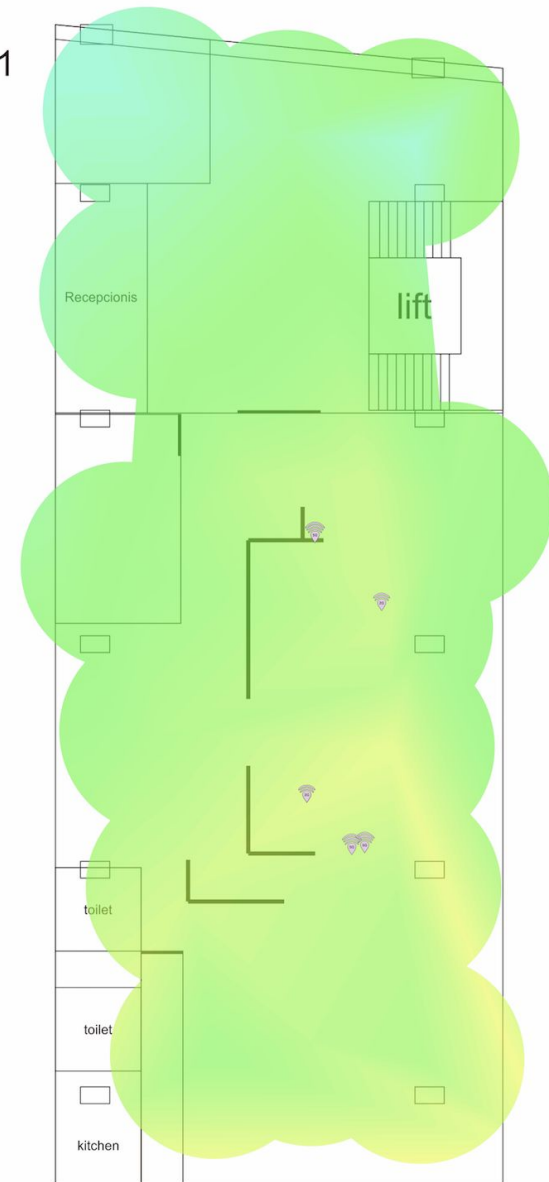




# Detecting rogue access point

- After all AP are integrated in capsman,
- CAPsMAN can detect a rogue AP in wireless network
- The dude integration?

FLOOR 1  
1:100

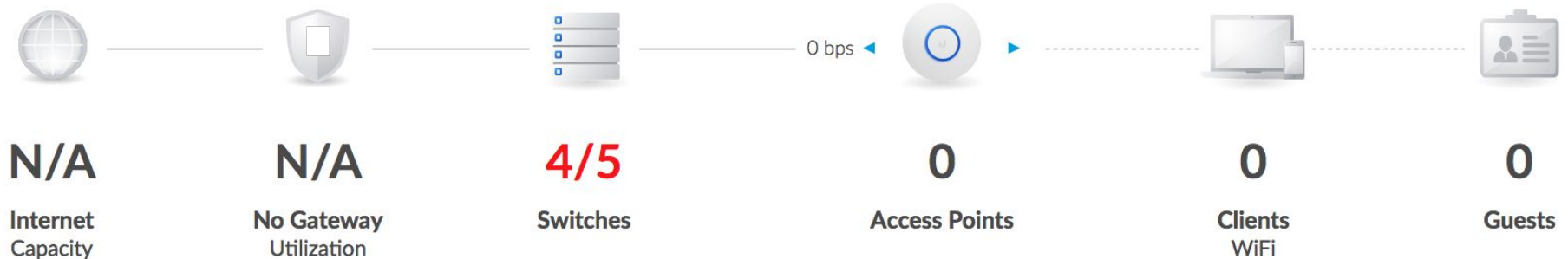


# EAP support on usermanager

- Currently EAP support is not available on Mikrotik Usermanager
- We use other radius software for EAP authentication
- Perhaps in the future?

# Complete controller application

- One centralised application to control / monitor devices:
  - Access point
  - Switch
  - Router
- Single dashboard for all devices
- Very useful for troubleshooting. E.g. to find a rogue DHCP server



# Training topics

- Previously, mikrotik wireless product was focusing on outdoor environment, Point-To-Point / Point-To-Multi-Point
- Since CAPsMAN appears, mikrotik is also focusing on indoor wireless
- Suggestion for the training track:
  - Mikrotik certified **outdoor** wireless engineer, focusing on outdoor wireless application
  - Mikrotik certified **enterprise** wireless engineer, focusing on indoor implementation with CAPsMAN

# Interested? Just come to our training...

- **Check schedule on our website**
- More hands-on
- Not only learn the materials, but also sharing experiences, best-practices, and networking

The screenshot shows a web browser displaying the 'Schedule' page of the GLC Networks website. The URL is <https://www.glcnetworks.com/schedule/>. The page features a navigation menu with 'HOME', 'PRODUCT', 'SCHEDULE', 'GALLERY', 'JOB', 'CONTACT', and 'BLOG'. A search bar is located below the navigation. The main content is organized by month:

- Nov 2017**
  - [FREE] Webinar: Policy Based Routing with Mikrotik
- Dec 2017**
  - MTCNA Training in Bandung (4-6 December 2017)
  - Workshop "BGP Routing"
  - MTCNA + MTCRE Training in Auckland (11-16 December 2017)
  - [FREE] Webinar: Load balancing with PCC
  - MTCNA + MTCRE Training in Lombok (18 - 23 December 2017)
  - Training CentOS System Administration, Jakarta, (26-30 December 2017)
  - [FREE] Webinar: OSPF on Mikrotik
- Jan 2018**
  - MTCINE Training in Jakarta (8-11 January 2018)
  - [FREE] Webinar: topic to be announced
  - MTCNA Training in Manila (13-15 January 2018)
  - MTCNA + MTCRE in Bandung (22-27 January 2018)

On the right side of the page, there are sections for 'Upcoming events' and 'Recent Posts'. The 'Upcoming events' section lists:

- [FREE] Webinar: Policy Based Routing with Mikrotik
- MTCNA Training in Bandung (4-6 December 2017)
- Workshop "BGP Routing"
- MTCNA + MTCRE Training in Auckland (11-16 December 2017)
- [FREE] Webinar: Load balancing with PCC

The 'Recent Posts' section lists:

- Nearest Events - MTCNA + MTCRE Lombok
- Nearest Events - MTCNA Bandung

QA

End of slides

