Build enterprise wireless with **CAPsMAN**

Mikrotik User Meeting Yogyakarta,
October 19-20, 2018

Achmad Mardiansyah
achmad@glcnetworks.com
GLC Networks, Indonesia
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)
- 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, mikrotik.tips, 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, Bussiness 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

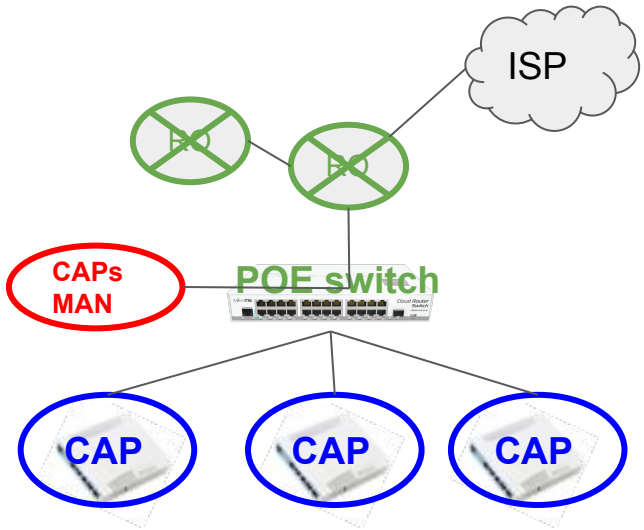
About CAPsMAN

- 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

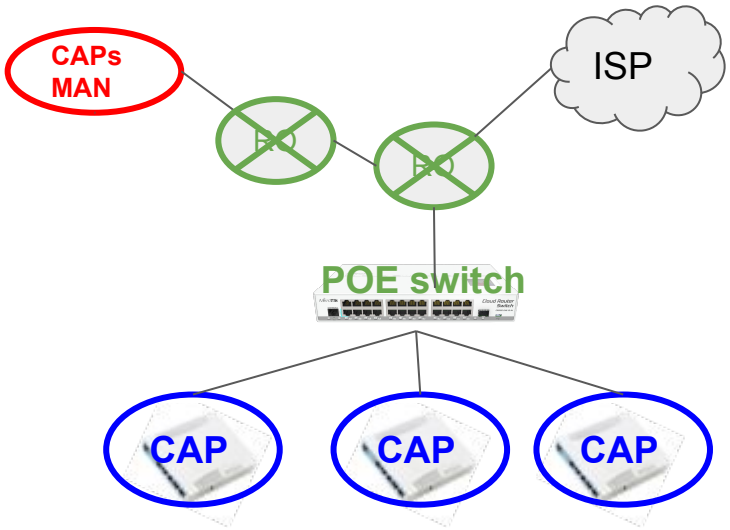
Layer 2

- CAP and CAPsMAN are in the same network

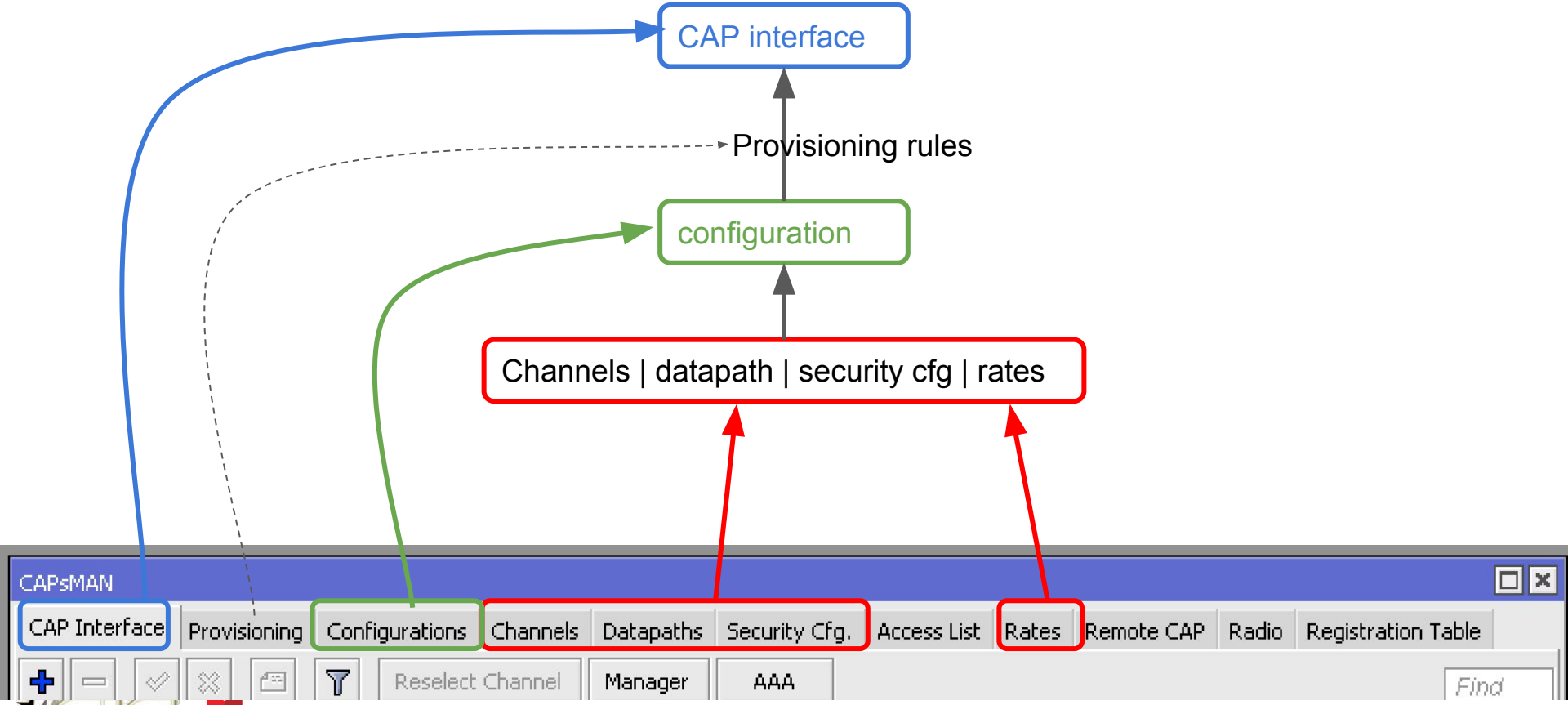


Layer 3 (recomm.)

- CAP and CAPsMAN are in different network



CAPsMAN configuration concepts



Channels | datapath | security cfg | rates

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

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

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 | Rat

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

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: master-AP1
Mode: ap
SSID: OneVision
Hide SSID:
Load Balancing Group: floor1-OneVision-2ghz
Distance: indoors km
Hw. Retries: 4
Hw. Protection Mode:
Frame Lifetime:
Disconnect Timeout:
Keepalive Frames:
Country: indonesia
Max Station Count:
Multicast Helper: disabled
HT Tx Chains: ☑ 0 ☑ 1 ☑ 2
HT Rx Chains: ☑ 0 ☑ 1 ☑ 2
HT Guard Interval: any

Wireless | Channel | Rates | Datapath | Security

Rate: rate-default
Basic Rates
Supported Rates
HT Basic MCS
HT Supported MCS
VHT Basic MCS
VHT Supported MCS

Wireless | Channel | Rates | Datapath | Security

Security: wpa-psk-old
Authentication Type:
Encryption:
Group Encryption:
Group Key Update:
Passphrase:
EAP Methods:
EAP Radius Accounting:
TLS Mode:
TLS Certificate:

Wireless | Channel | Rates | Datapath | Security

Channel: f-2412
Frequency:
Control Channel Width:
Band:
Extension Channel:
Tx Power:
Save Selected:
Reselect Interval:
Skip DFS Channels:

Wireless | Channel | Rates | Datapath | Security

Datapath: dp-lf
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:

OK | Cancel | Apply | Disable | Comment | Copy | Remove

enabled

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:

OK | Cancel | Apply | Disable | Comment | Copy | Remove

enabled

Master vs slave configuration

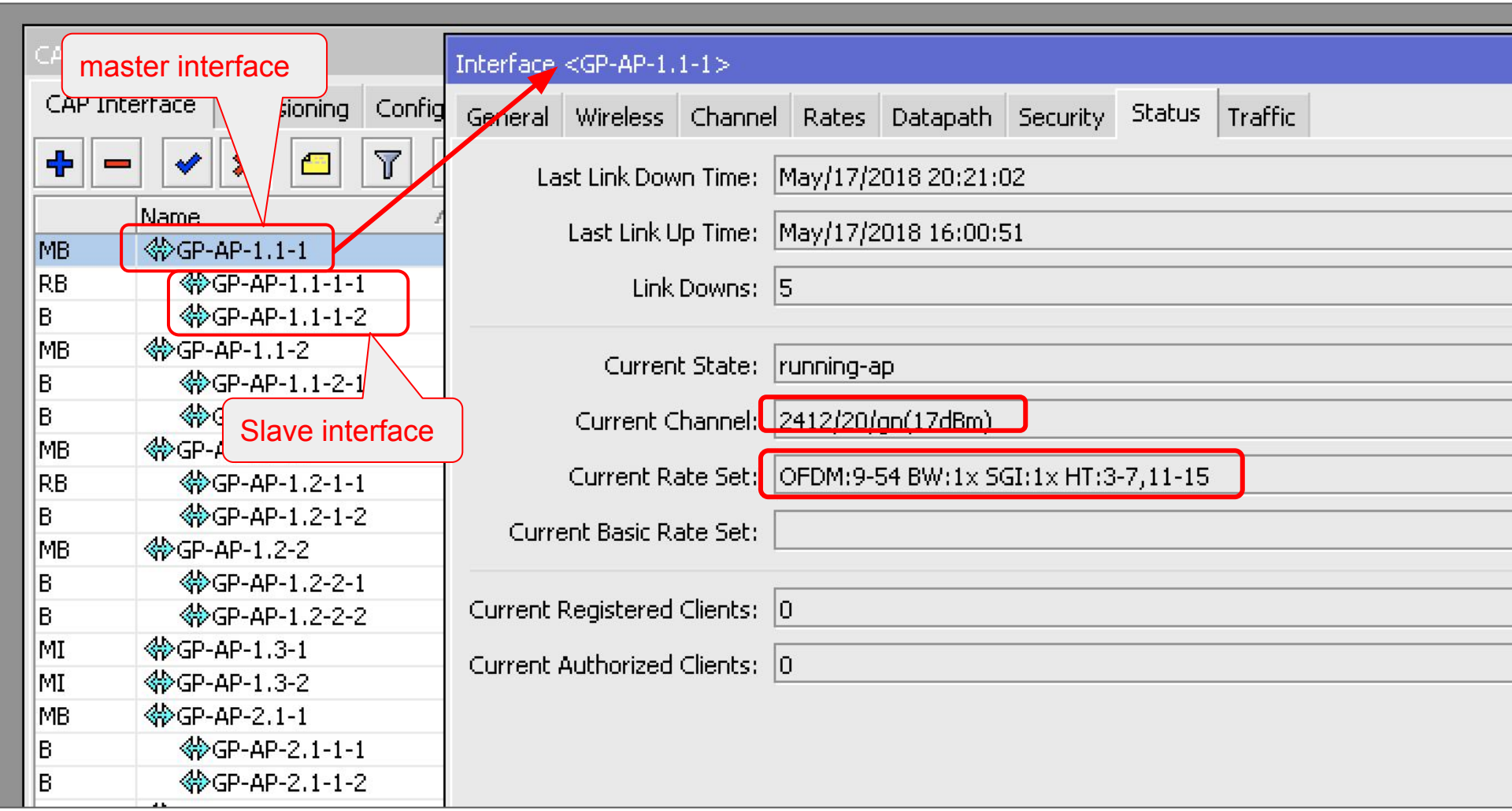
Master

- 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



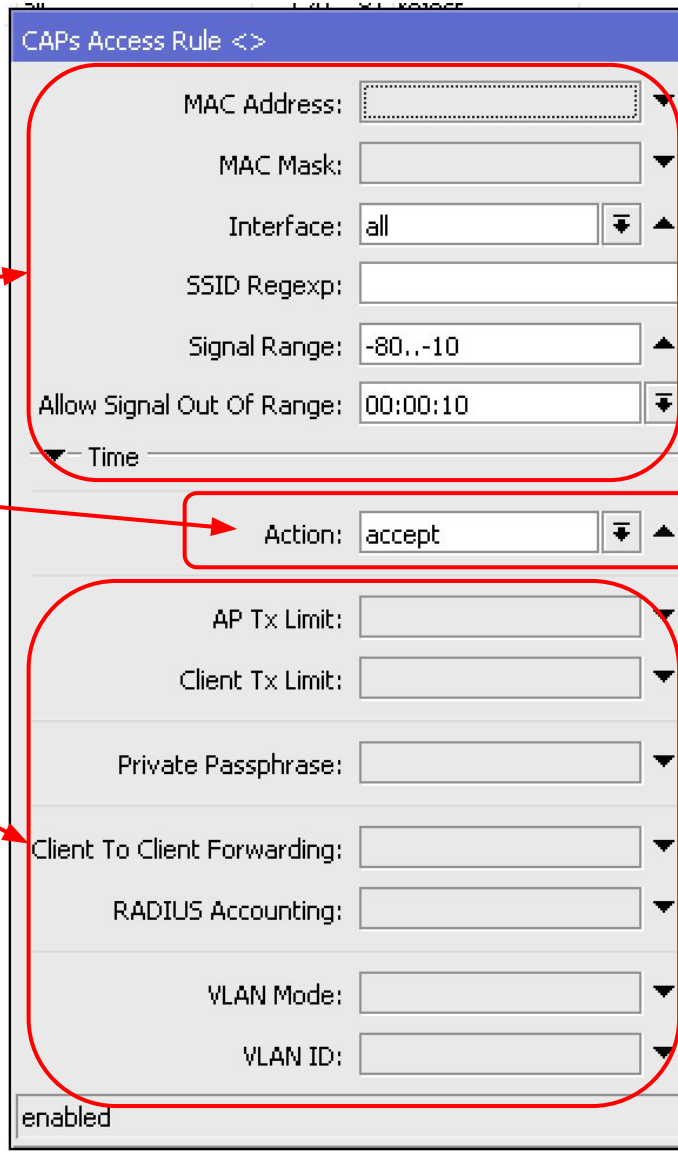
CAPsMAN features

Access list

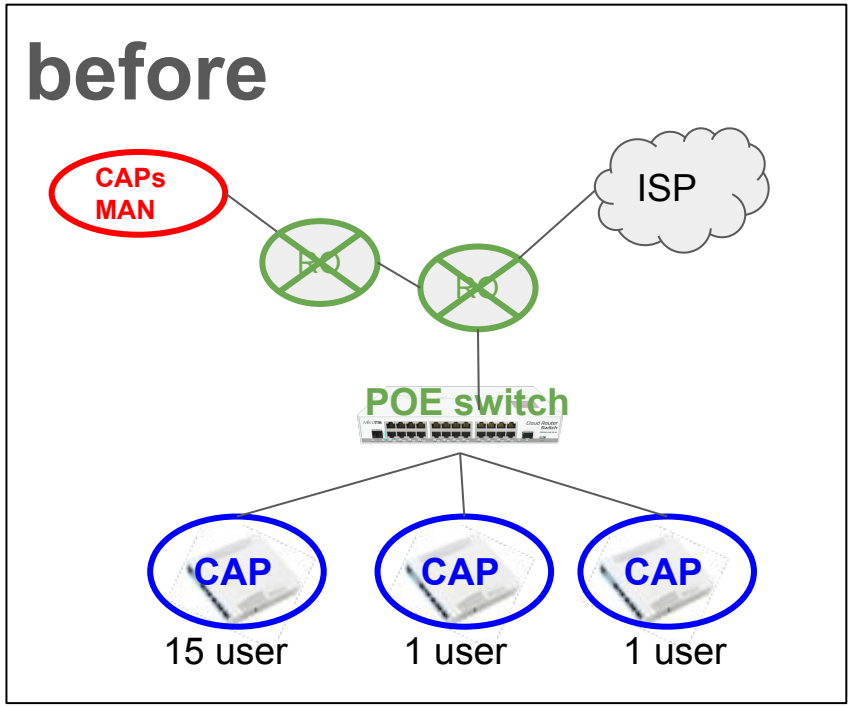
- Is used to control wifi access
- Format:
  - Client matching
  - Action:
    - accept | reject | query radius
  - Connection parameter

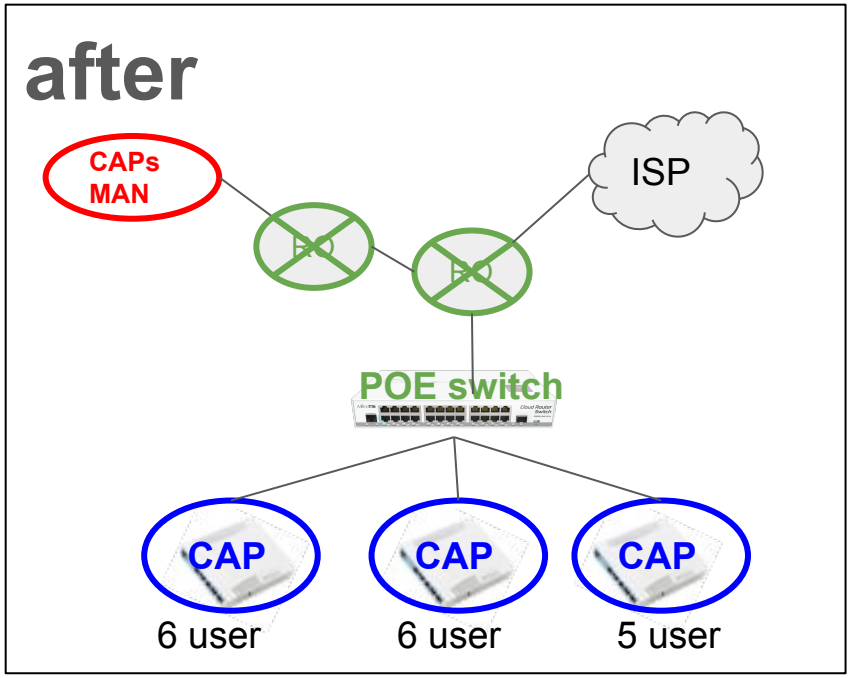
Notes:

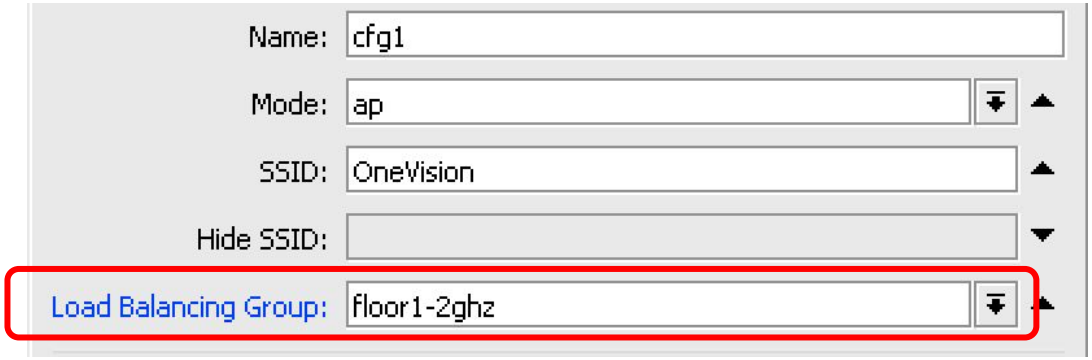
- **Client tx limit** is for mikrotik devices only



Load balancing AP

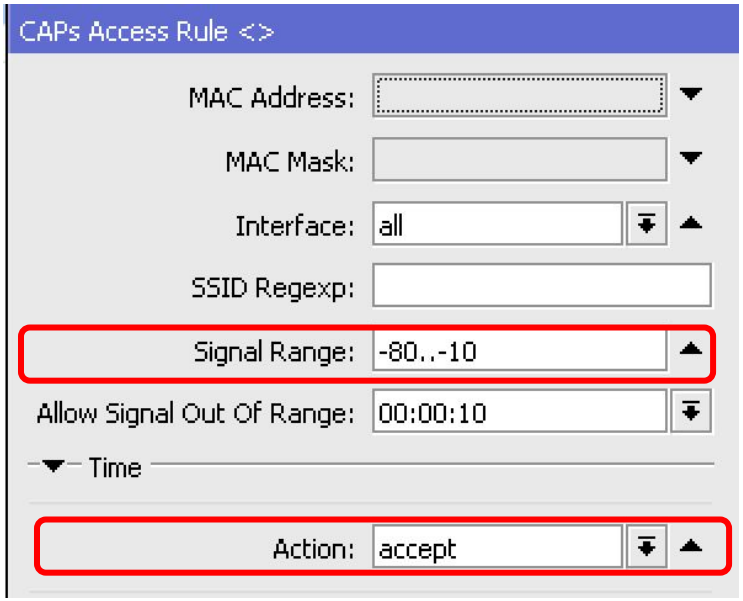


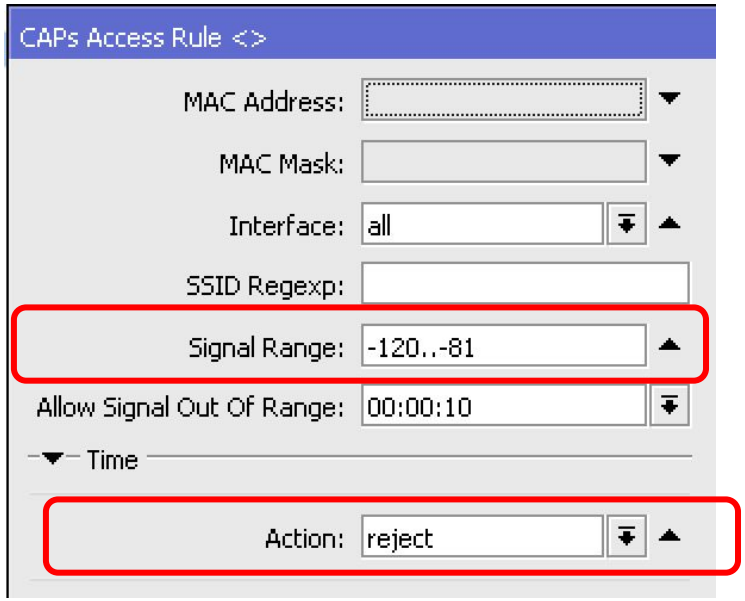




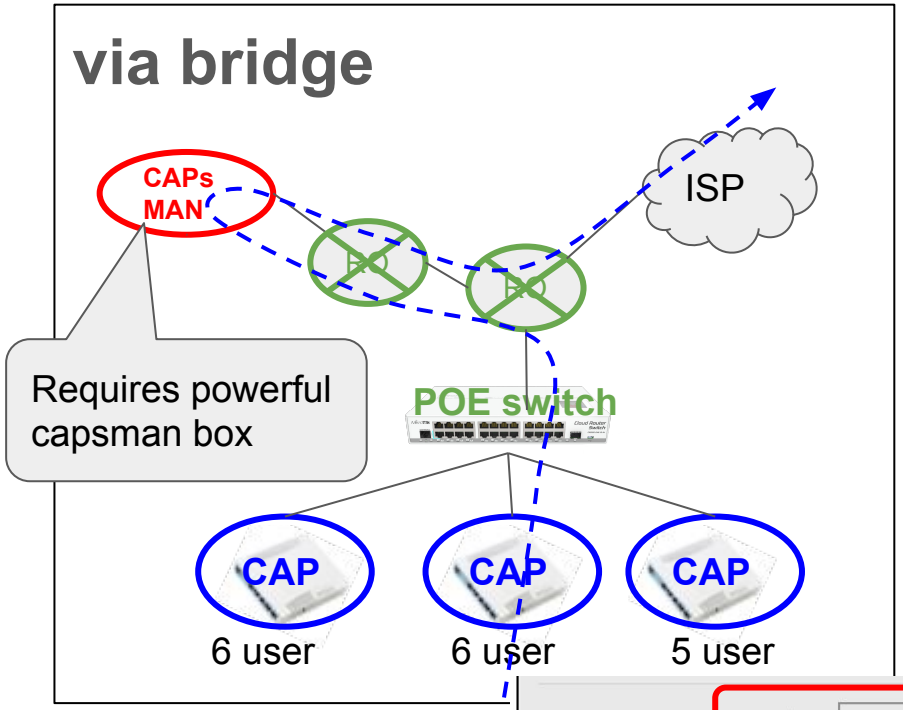
Roaming

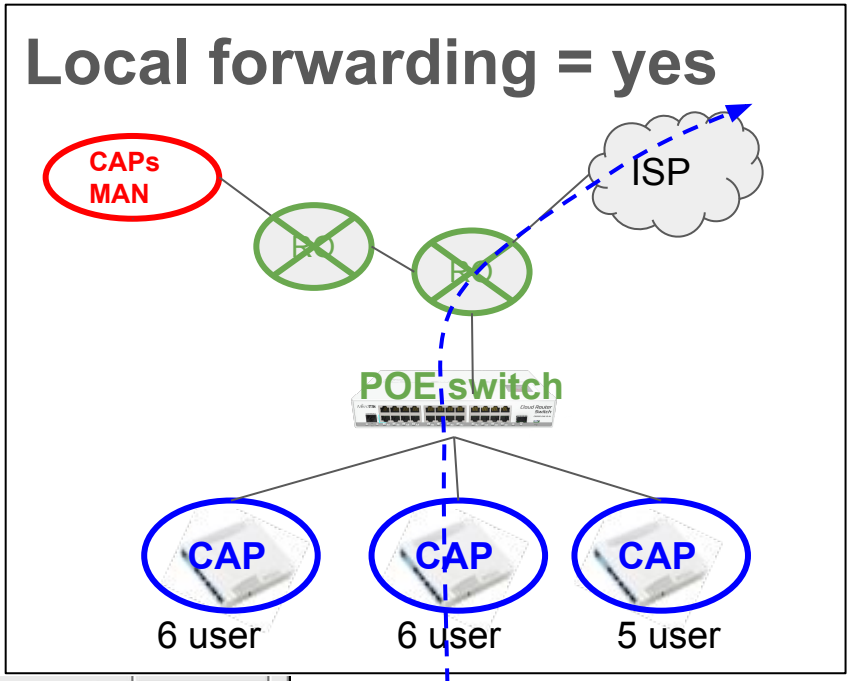
- Unlike GSM, connection to AP is end-user decision, not AP.
- Often, station is **still attached to old AP** even though already moved to new AP
- What AP can set up a threshold for disassociation (based on signal level)
- On CAPsMAN, we use **access rule**

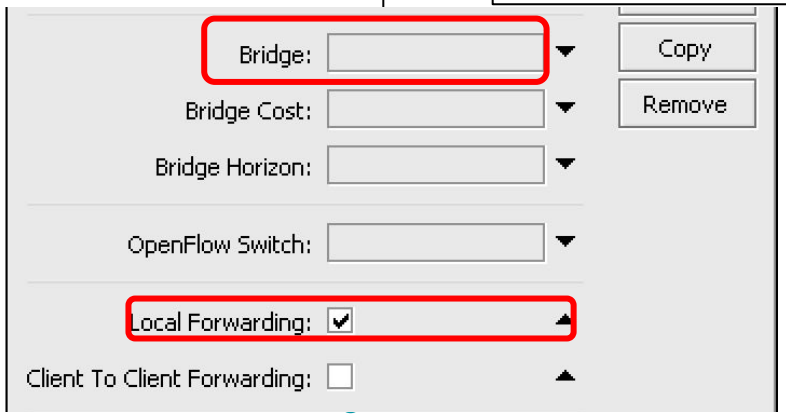




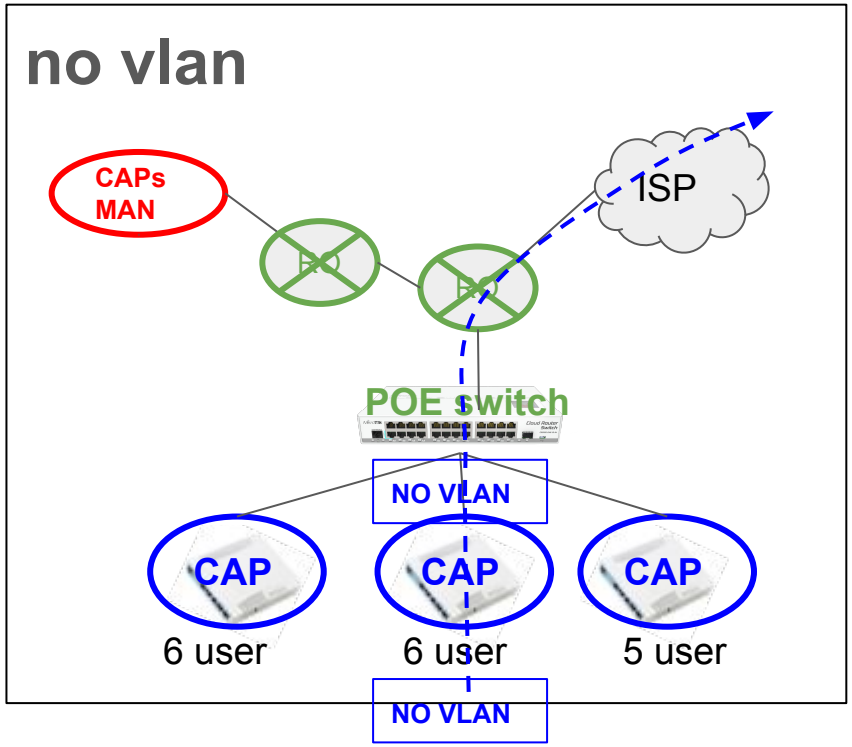
Datapath (local forwarding)

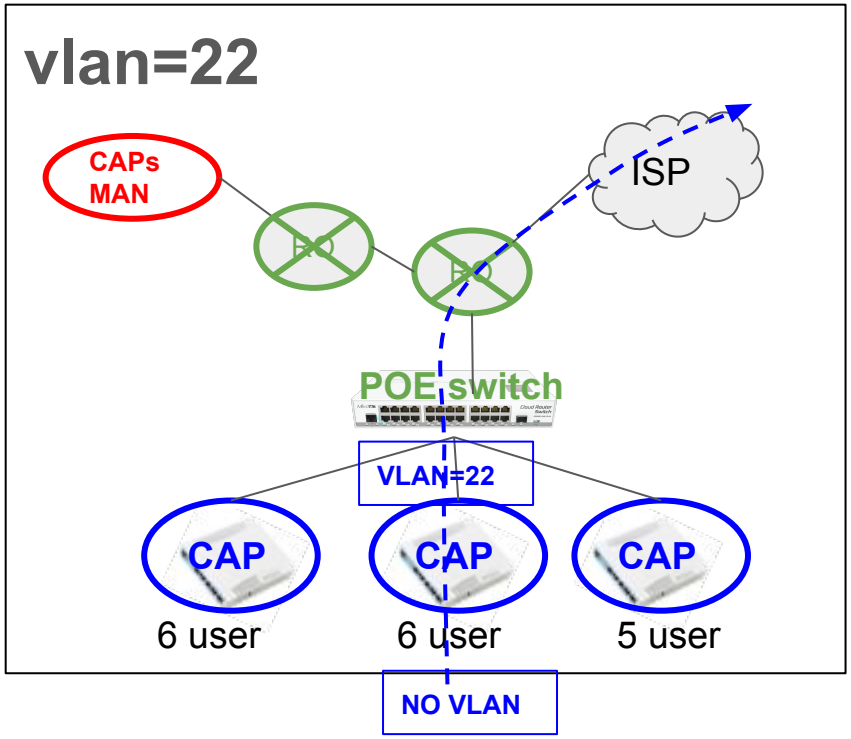


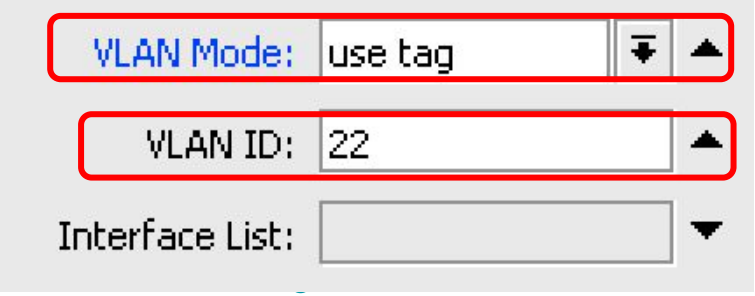




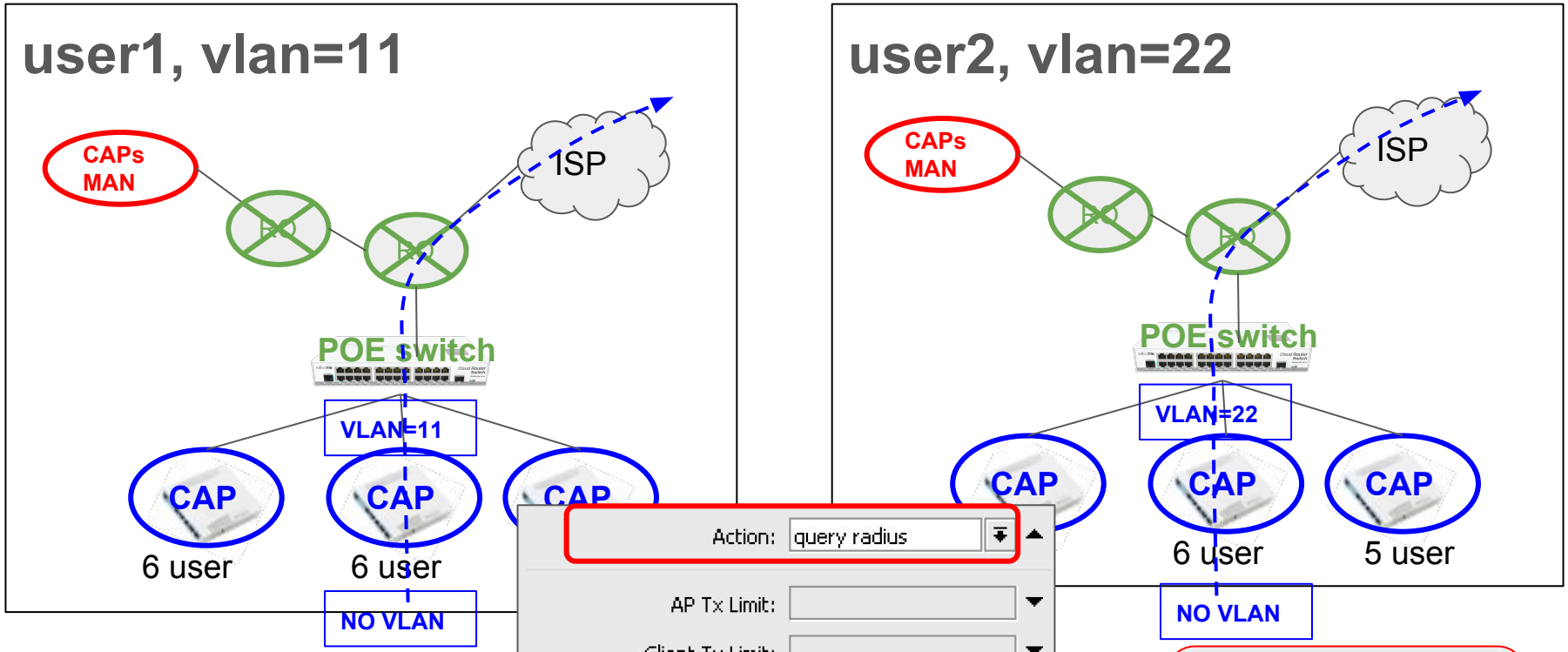
Datapath (vlan)

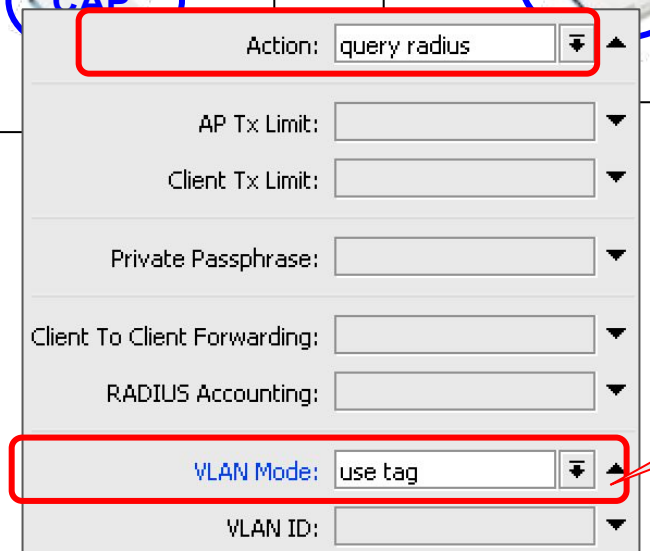






Datapath (vlan per user)

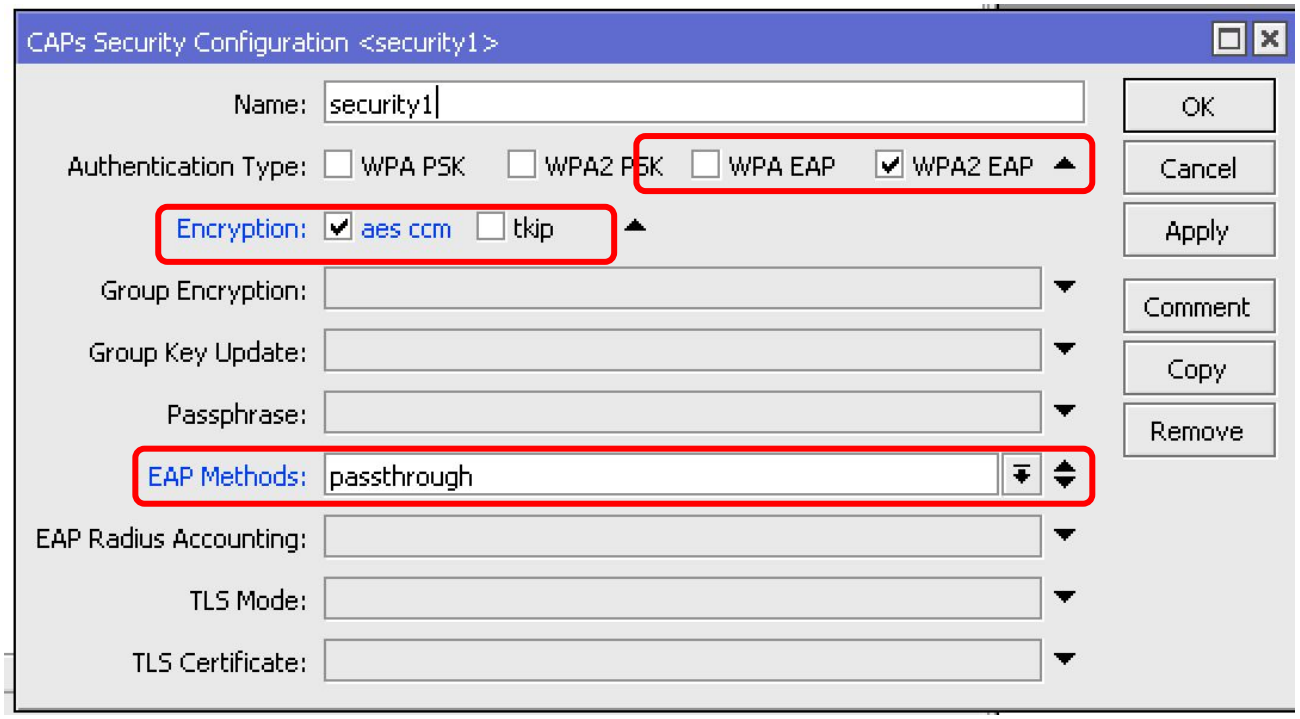




Need support from radius server which provides vendor attribute

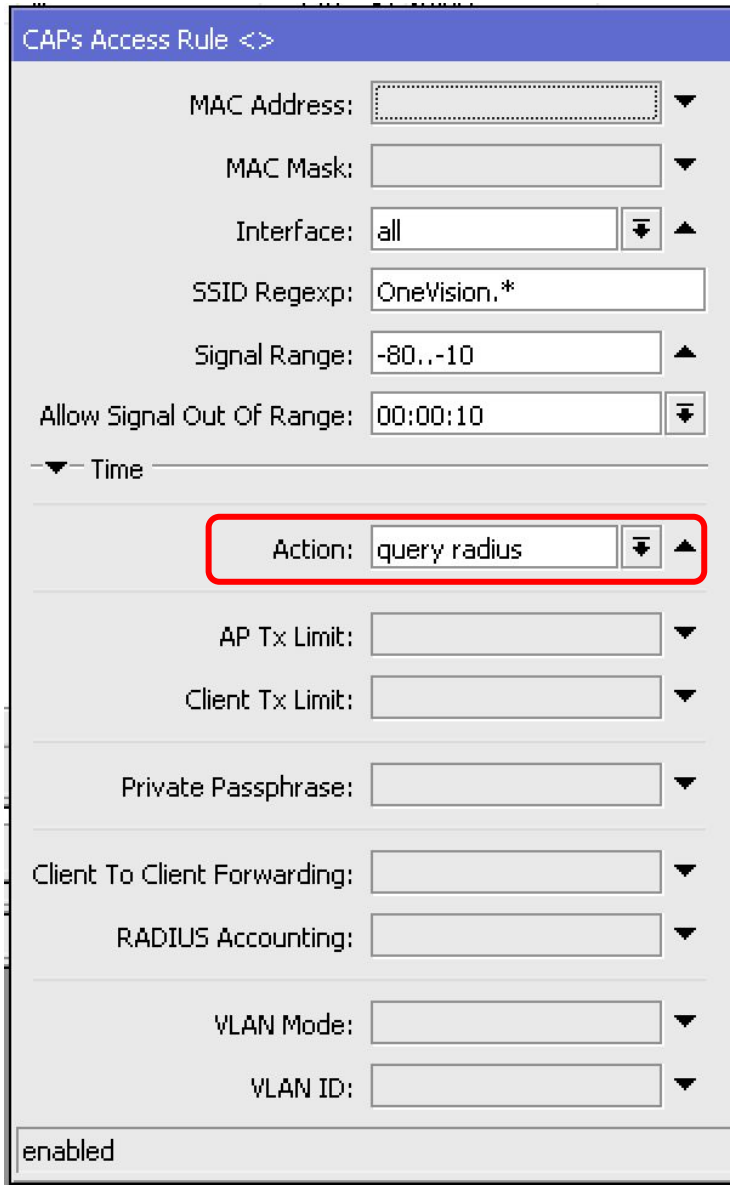
Security: EAP (layer 2 authentication)

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



MAC based authentication

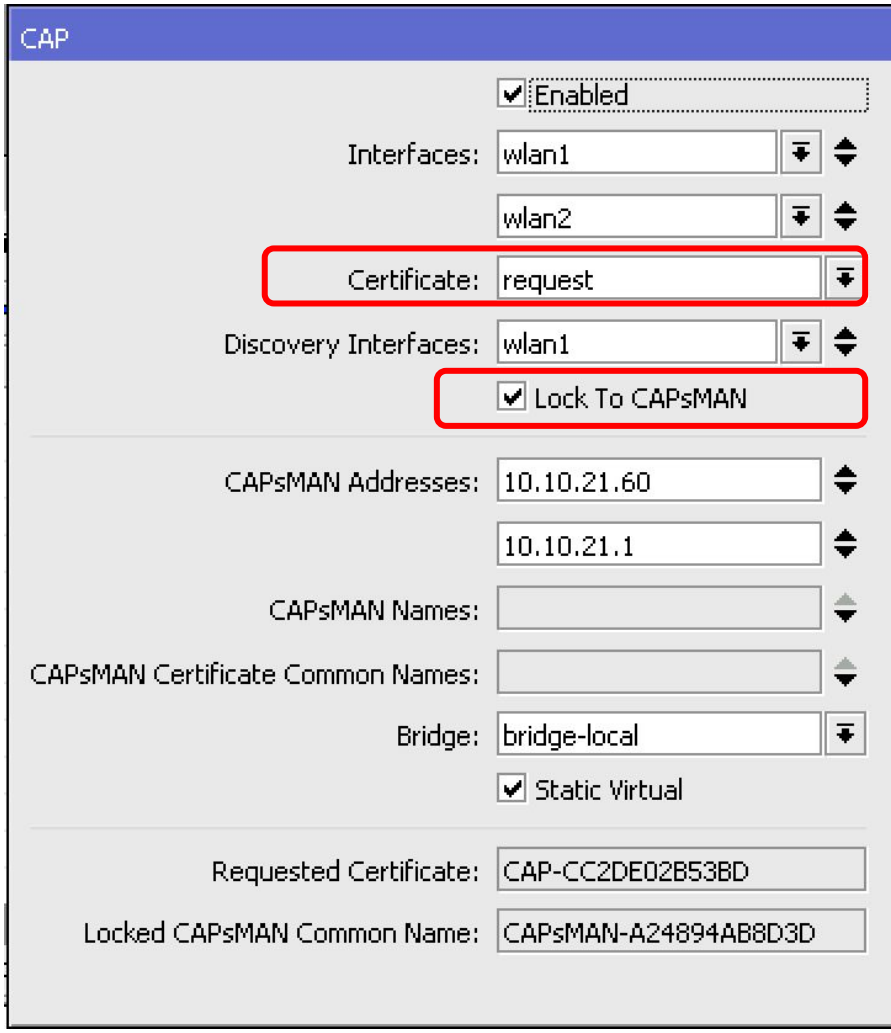
- It is possible to allow client to connect based on MAC address
- We need support from radius server which contains MAC address database
- Combined with access-list



CAPsMAN tips

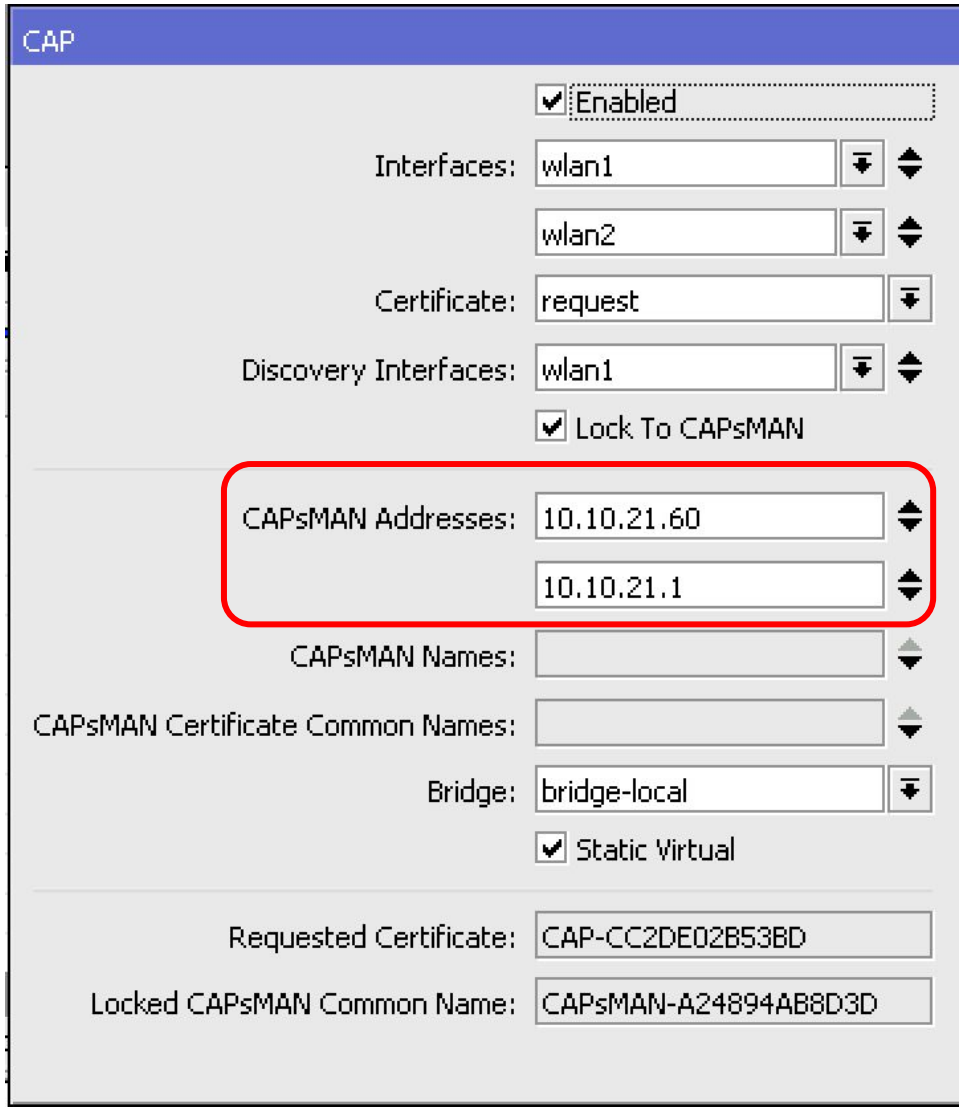
CAP: use auto certificate

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



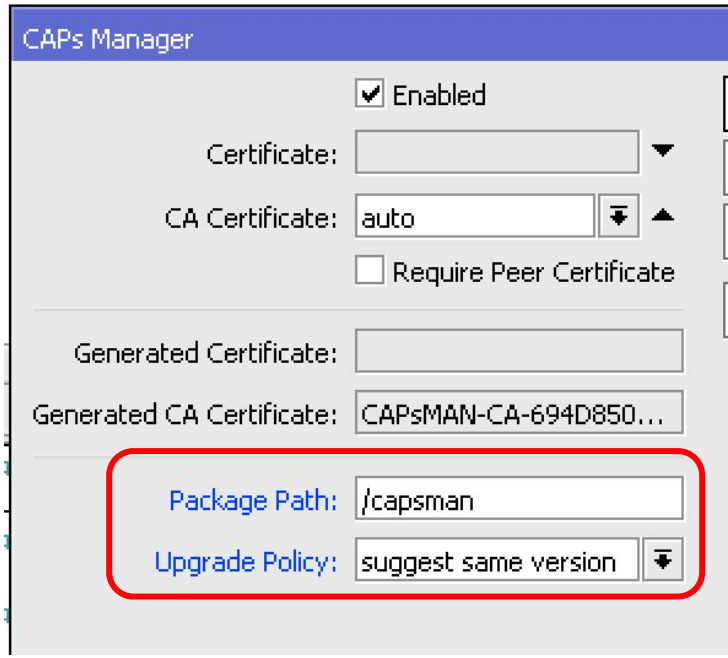
CAP: high availability

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



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

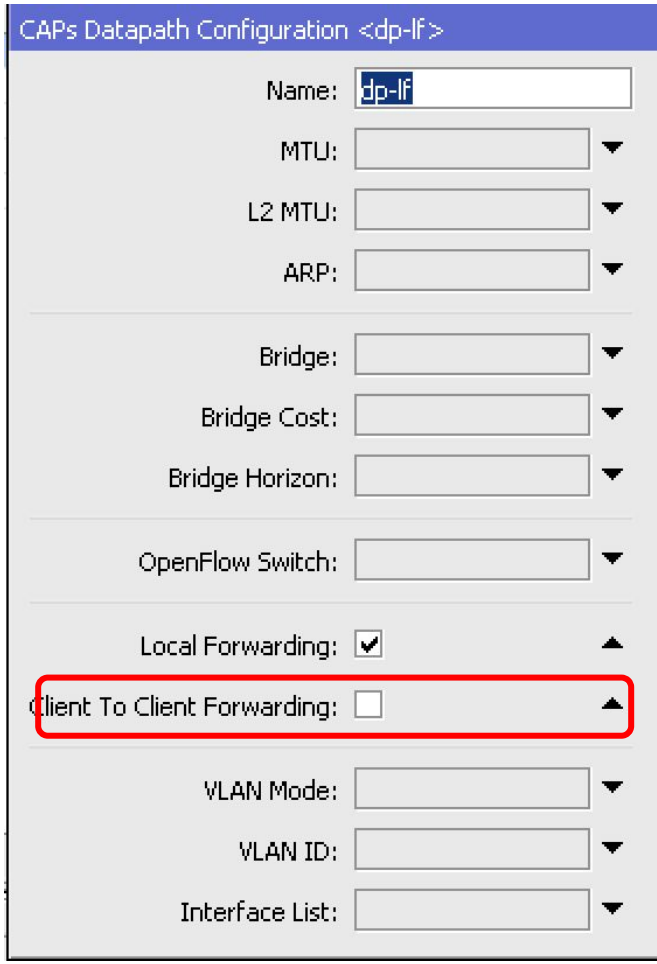


Wireless survey

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

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

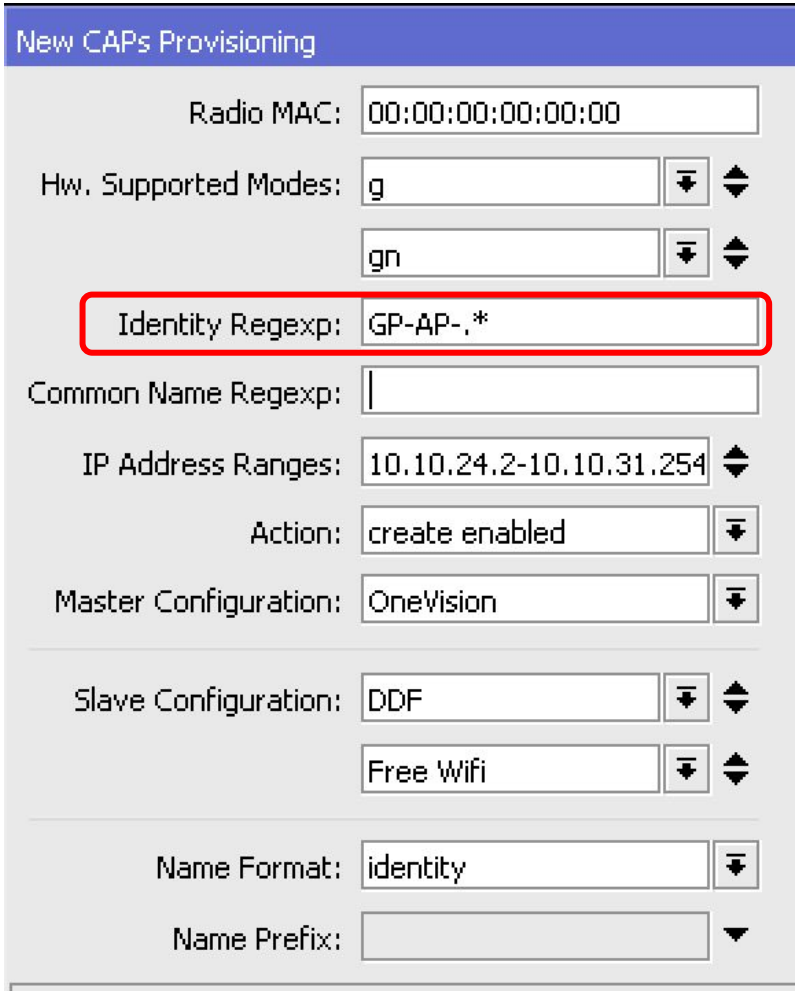


Smooth mobility for client

- 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

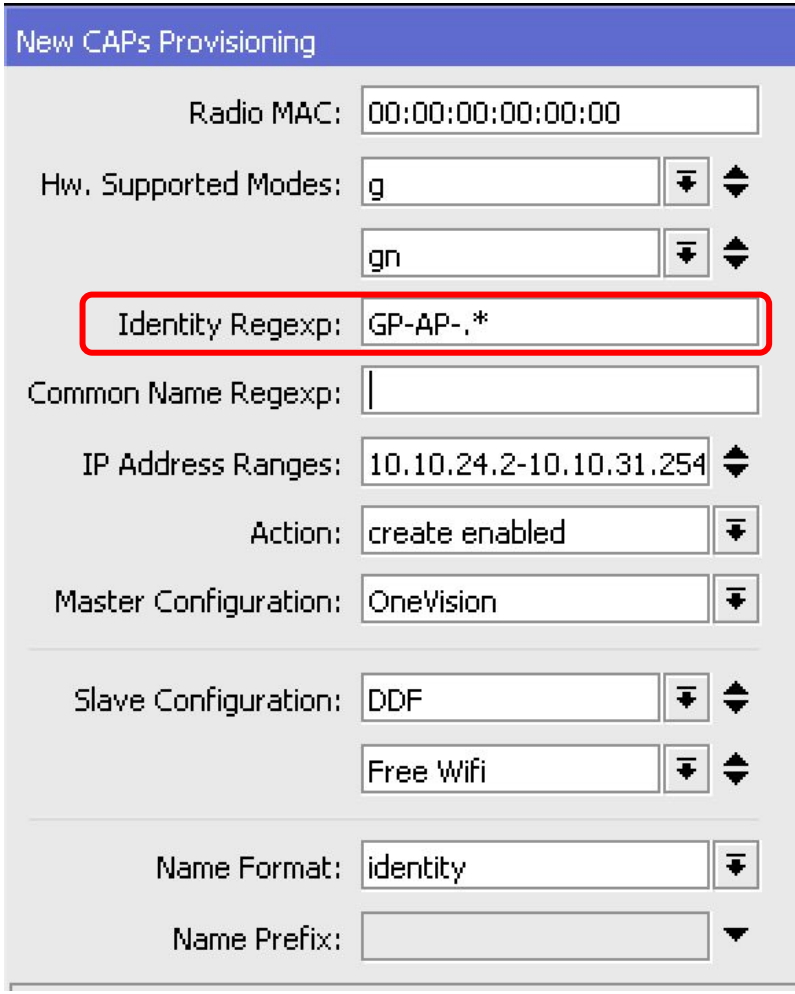
Flexible provisioning

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



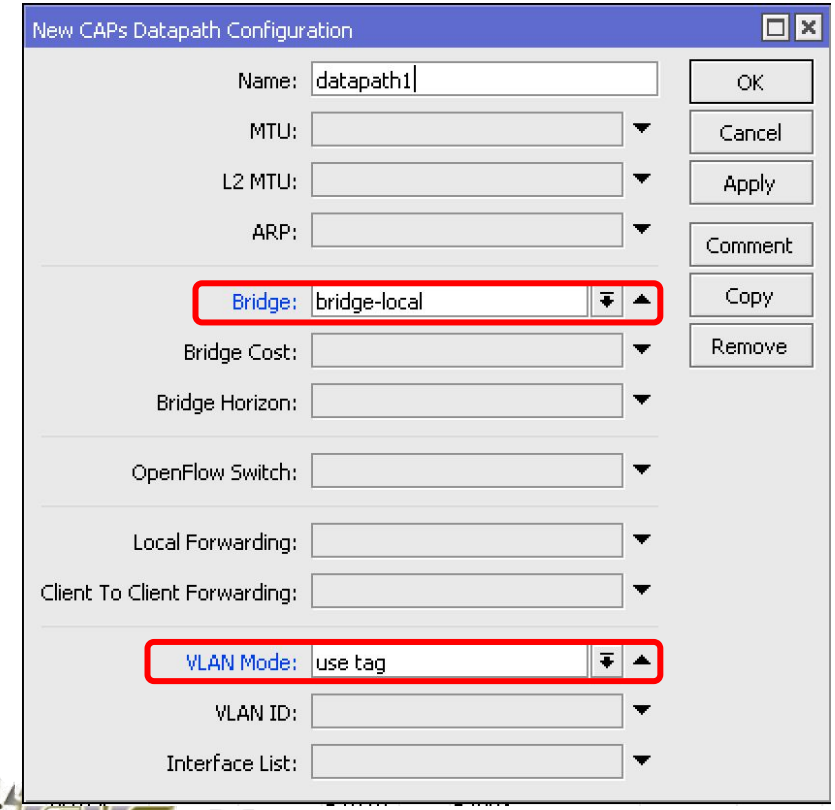
Flexible provisioning

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



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




```
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       Mikortik_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 are encourage users to connect to 5GHz band as its less crowed compared to 2GHz band
- Currently its 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?

Detecting rogue access point

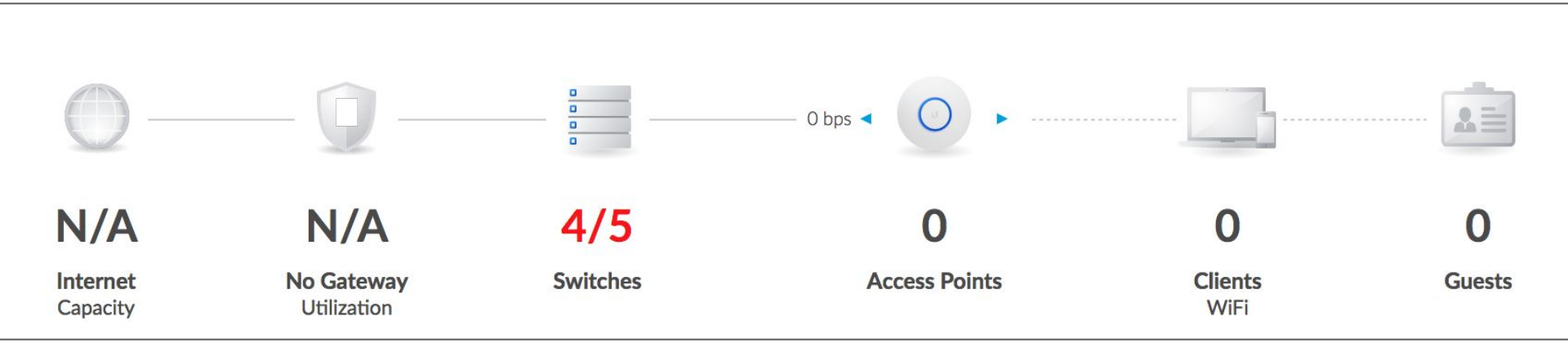
- After all AP are integrated in capsman,
- CAPsMAN can detect a rogue AP in wireless network
- Thedude integration?

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

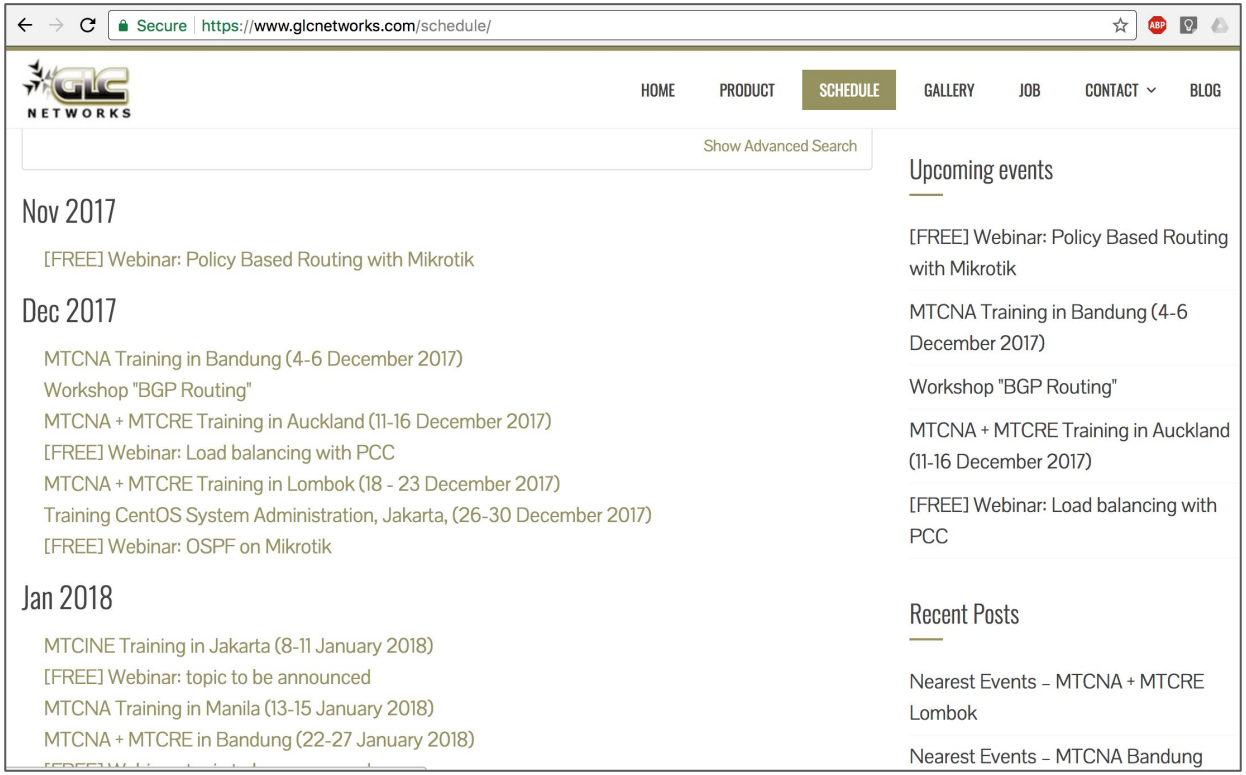


Training topics

- 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



www.glcnetworks.com

QA

End of slides