

MUM Kyiv 2018

CAPsMAN. Практическая реализация и неочевидные особенности.

Шишко Александр
shaman-mail@ukr.net
[LinkedIn Profile](#)

CAPsMAN

- Коротко о себе.
- На кого рассчитана доклад?
- О чем доклад?

Беглый обзор интерфейса CAPsMAN

Интерфейс логически делится на 3 части:

Interfaces - Configuration - Info

Настраивается с конца.

Если не заработало:

Включить контроллер кн. Manager -> Enabled
Discovery-interfaces

Безопасность. Аутентификация по сертификату.
ИБ как образование, она либо есть либо ее нет.

The screenshot displays the CAPsMAN interface with the following components:

- Top Bar:** CAPsMAN title bar and a menu bar with tabs: CAP Interface, Provisioning, Configurations, Channels, Datapaths, Security Cfg., Access List, Rates, Remote CAP, Radio, and Registration Table. The 'CAP Interface' tab is highlighted with a red box.
- Table:** A table listing configured CAP interfaces. The table has columns: Name, Type, Tx, Rx, Tx Pac..., Rx Pa..., Configuration, and SSID. The data is as follows:

Name	Type	Tx	Rx	Tx Pac...	Rx Pa...	Configuration	SSID
MB zcap-MT-HomeAP-1	CAP Interface	0 bps	0 bps	0	0	W1	W1
SB zcap-MT-HomeAP-1-1	CAP Interface	0 bps	0 bps	0	0	W1Hotspot	W1_Hotspot
MB zcap-MT-HomeAP-5Hz-W1	CAP Interface	0 bps	0 bps	0	0	W1	W1
SB zcap-MT-HomeAP-5Hz-W1-Hotspot	CAP Interface	0 bps	0 bps	0	0	W1Hotspot	W1_Hotspot
RMB zcap-MT-SlaveAP-1	CAP Interface	0 bps	0 bps	0	0	W1	W1
RSB zcap-MT-SlaveAP-1-1	CAP Interface	0 bps	0 bps	0	0	W1Hotspot	W1_Hotspot
- CAPs Manager Dialog:** A dialog box with a title bar 'CAPs Manager'. It contains a checkbox 'Enabled' (checked and highlighted with a red box), fields for 'Certificate:', 'CA Certificate:', and 'Require Peer Certificate' (unchecked). It also has fields for 'Generated Certificate:', 'Generated CA Certificate:', 'Package Path:', and 'Upgrade Policy: none'. Buttons 'OK', 'Cancel', 'Apply', and 'Interfaces' are present.
- CAP Dialog:** A dialog box with a title bar 'CAP'. It contains a checkbox 'Enabled' (checked and highlighted with a red box), fields for 'Interfaces:' (wlan1, wlan2), 'Certificate:' (none), and 'Discovery Interfaces:' (vlan1-ros253-in, highlighted with a red box). It also has a checkbox 'Lock To CAPsMAN' (unchecked). Below these are fields for 'CAPsMAN Addresses:', 'CAPsMAN Names:', 'CAPsMAN Certificate Common Names:', 'Bridge:' (none), and a checked checkbox 'Static Virtual'. At the bottom are fields for 'Requested Certificate:' and 'Locked CAPsMAN Common Name:'.

Datapath

- Применение Local Forwarding (Иллюстрация The Dude)
- L2 vs L3

Wireless Tables

WiFi Interfaces W60G Station Nstreme Dual Access List Registration Connect List Security Profile

Wireless (IPQ4019)

Name	Type	Actual MTU	Tx	Rx	Tx Pa
--- managed by CAPsMAN					
--- channel: 2462/20-eC/gn(20dBm), SSID: W1, local forwarding					
RS wlan1	Wireless (IPQ4019)	1500	0 bps	0 bps	
--- managed by CAPsMAN					
--- SSID: W1_Hotspot, CAPsMAN forwarding					
DX wlan49	Virtual	1500	0 bps	0 bps	
--- managed by CAPsMAN					
--- channel: 5200/20-eCee/ac(20dBm), SSID: W1, local forwarding					
RS wlan2	Wireless (IPQ4019)	1500	0 bps	0 bps	0 0 CC:2D:E0
--- managed by CAPsMAN					
--- SSID: W1_Hotspot, CAPsMAN forwarding					
DX wlan48	Virtual	1500	0 bps	0 bps	0 0 CE:2D:E0

4 items out of 15

Bridge

Bridge Ports VLANs MSTIs Port MST Overrides Filters NAT Hosts MDB

Dynamic is yes

#	Interface	Bridge	Horizon	Priority (h...	Path Cost	Role	R
5 D	wlan2	bridge-hgw		80	10	designated port	
6 D	wlan1	bridge-hgw		80	10	designated port	

CAP

☒ Enabled

Interfaces: wlan1 wlan2

Certificate: none

Discovery Interfaces: bridge-ros253

☐ Lock To CAPsMAN

CAPsMAN Addresses:

CAPsMAN Names:

CAPsMAN Certificate Common Names:

Bridge: bridge-hgw

☐ Static Virtual

Requester

Locked CAPsMAN Co

CAPs Datapath Configuration <W1>

Name: W1

MTU:

L2 MTU:

ARP:

Bridge: bridge-hgw

Bridge Cost:

Bridge Horizon:

Local Forwarding: ☒

Client To Client Forwarding: ☒

VLAN Mode:

VLAN ID:

Interface List:

Datapath

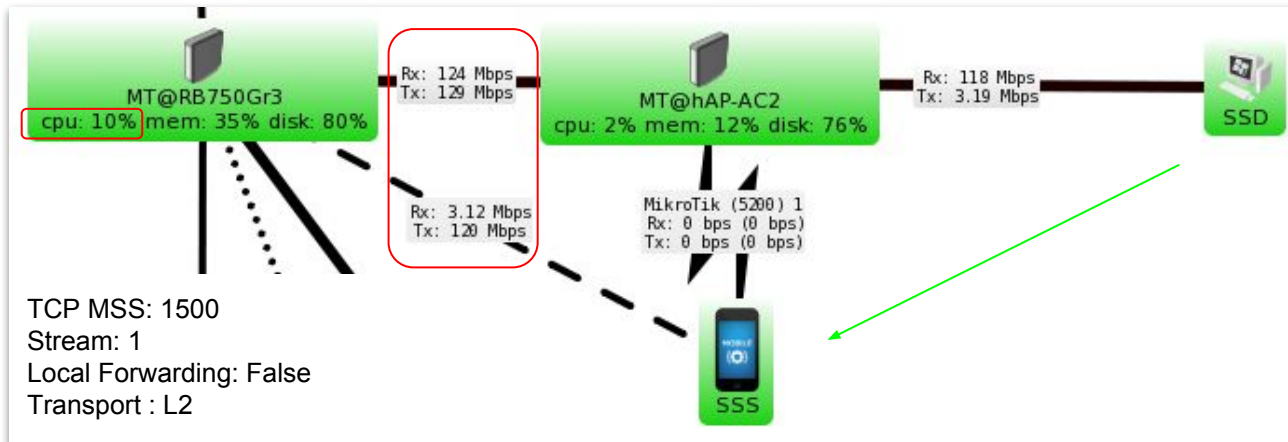
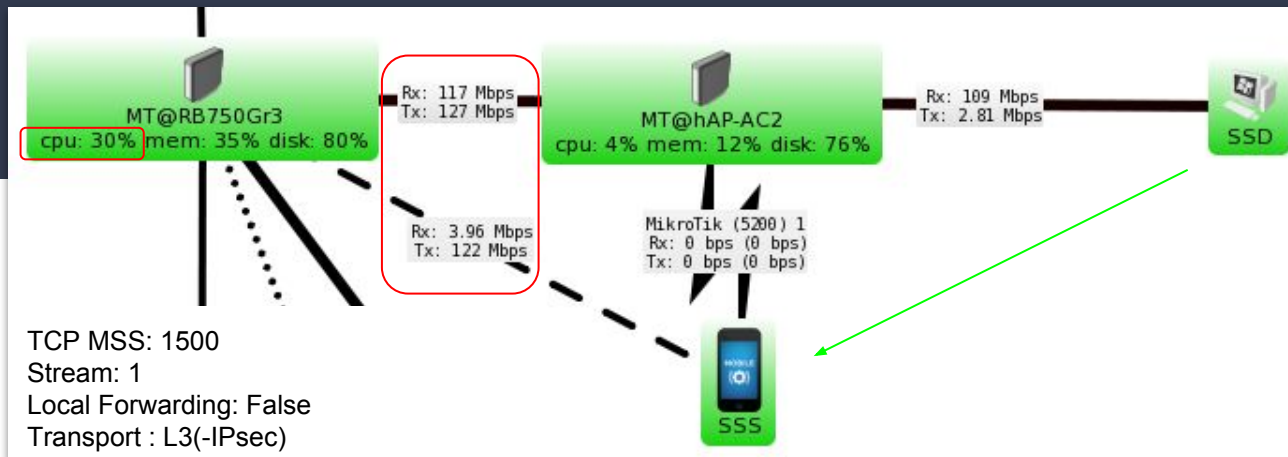
Хосты SSD и SSS входят в одноранговую сеть и находятся в L2 broadcast domain.

Нет плюсов/минусов. Есть особенности применения.

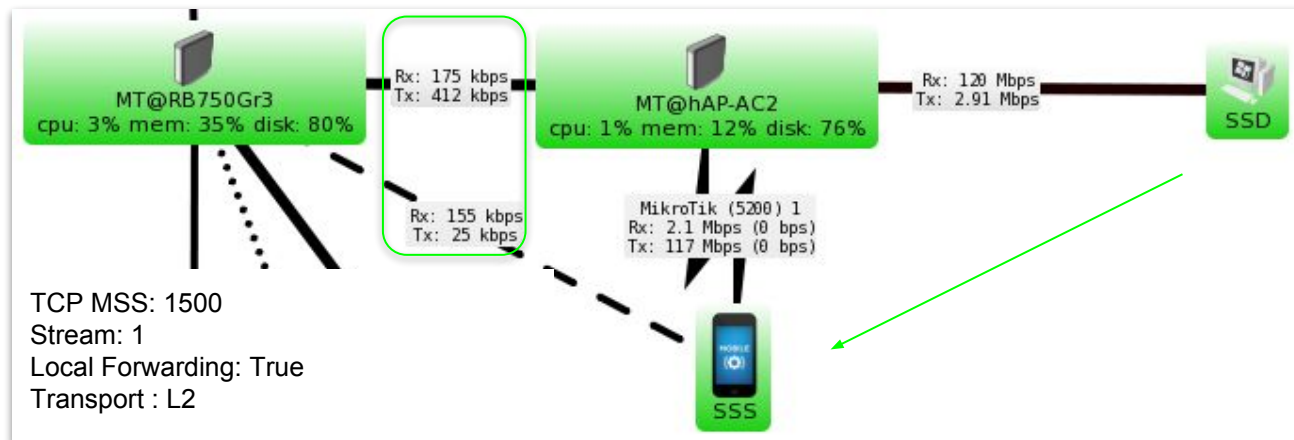
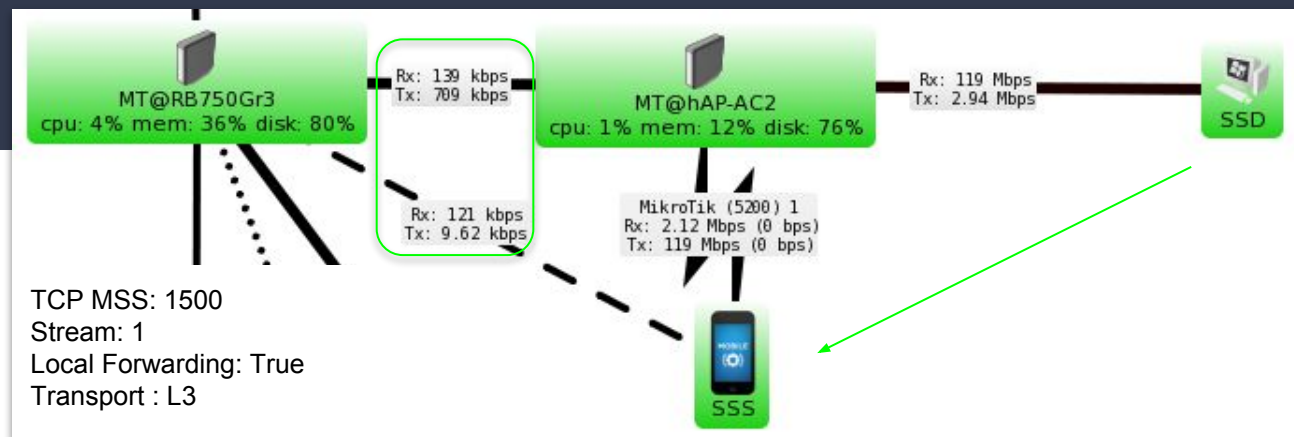
CAPsMAN не provision server.
Учитывая вышесказанное настоячиво рекомендую использовать CAPsMAN в пределах L2 broadcast domain

При включении LF и необходимости мониторить каналы можно использовать сторонние средства. Zabbix как вариант.

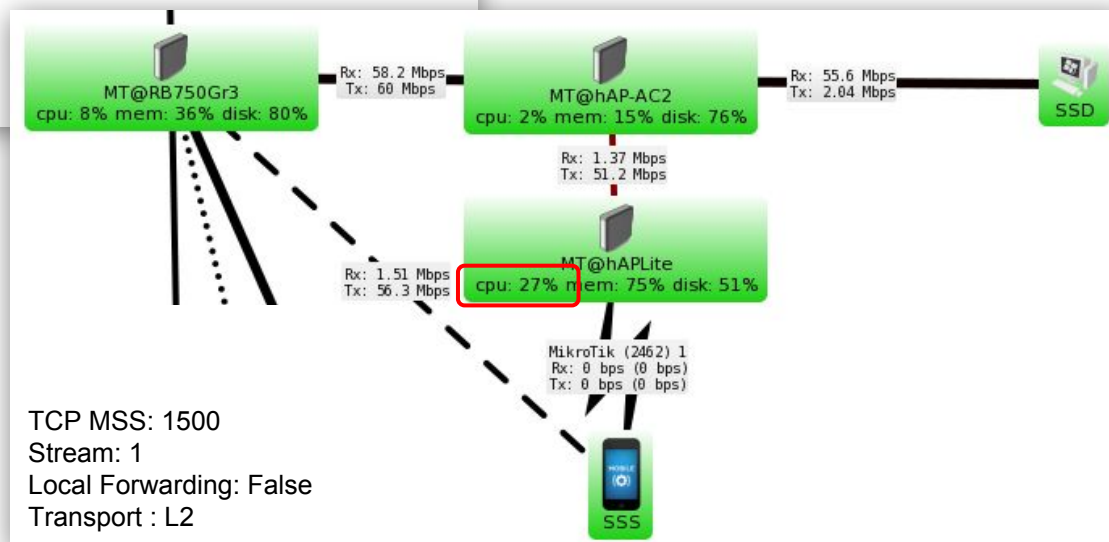
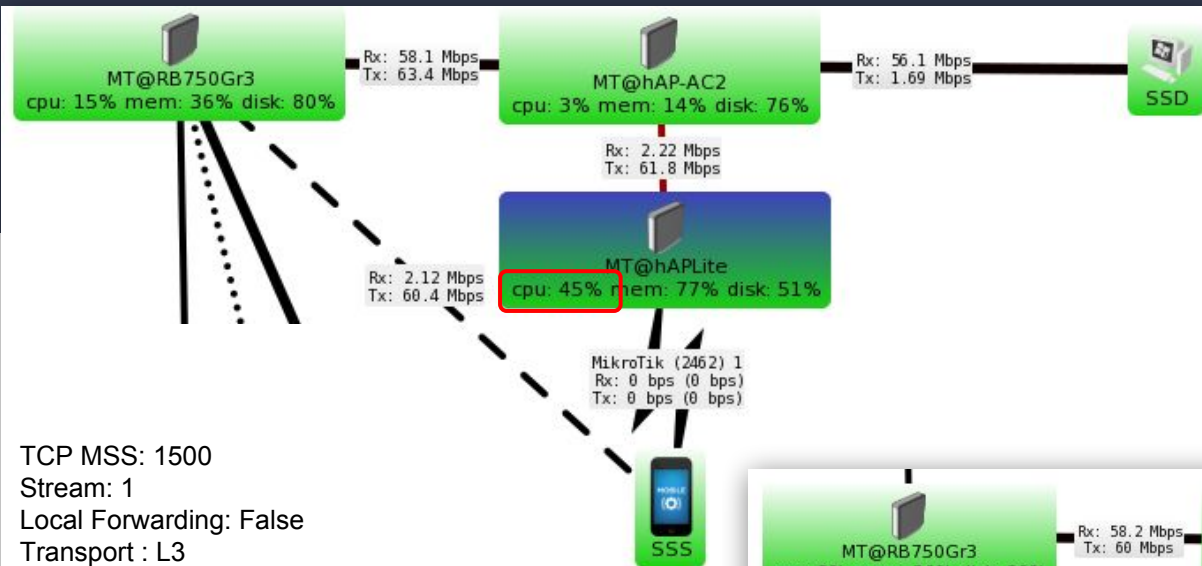
Можно не “тянуть” vlan`ы на все CAP`ы, и при необходимости натянуть IPsec(trans) при использовании IP транспорта.



Datapath



Datapath



ACL

- Fast BSS transition. 802.11r/k/v.

Чего делать не нужно:

Фильтрация по Signal Range

Что нужно знать:

Радиоэфир нестабильная среда.
disconnected, extensive data loss
disconnected, too weak signal

- Клиент сам выбирает где ему хорошо.
- Особенности реализации клиентских устройств.
- ACL - Конвейер
- Комментарии в ACL -> Reg. Table
- "Бесшовный роуминг" и CAPsMAN.
О Mesh + WDS поговорим в другой раз.
Ссылка в конце.

The screenshot displays the CAPsMAN web interface. The top navigation bar includes tabs for CAP Interface, Provisioning, Configurations, Channels, Datapaths, Security Cfg., Access List, Rates, Remote CAP, Radio, and Registration Table. The 'CAPs Scanner' tab is active, showing a table with columns: Interface, SSID, MAC Address, EAP Identity, Tx Rate, and Rx Rate. The interface 'zcap-MT-SlaveAP-1' is selected, and a context menu is open with options: Show Categories, Detail Mode, Inline Comments, Show Columns, Find (Ctrl+F), Find Next (Ctrl+G), and Copy to Access List. To the right, a table shows signal and uptime data:

Tx Signal	Rx Signal	Uptime
0	-57	00:19:48.17
0	-49	00:20:01.14
0	-46	00:20:02

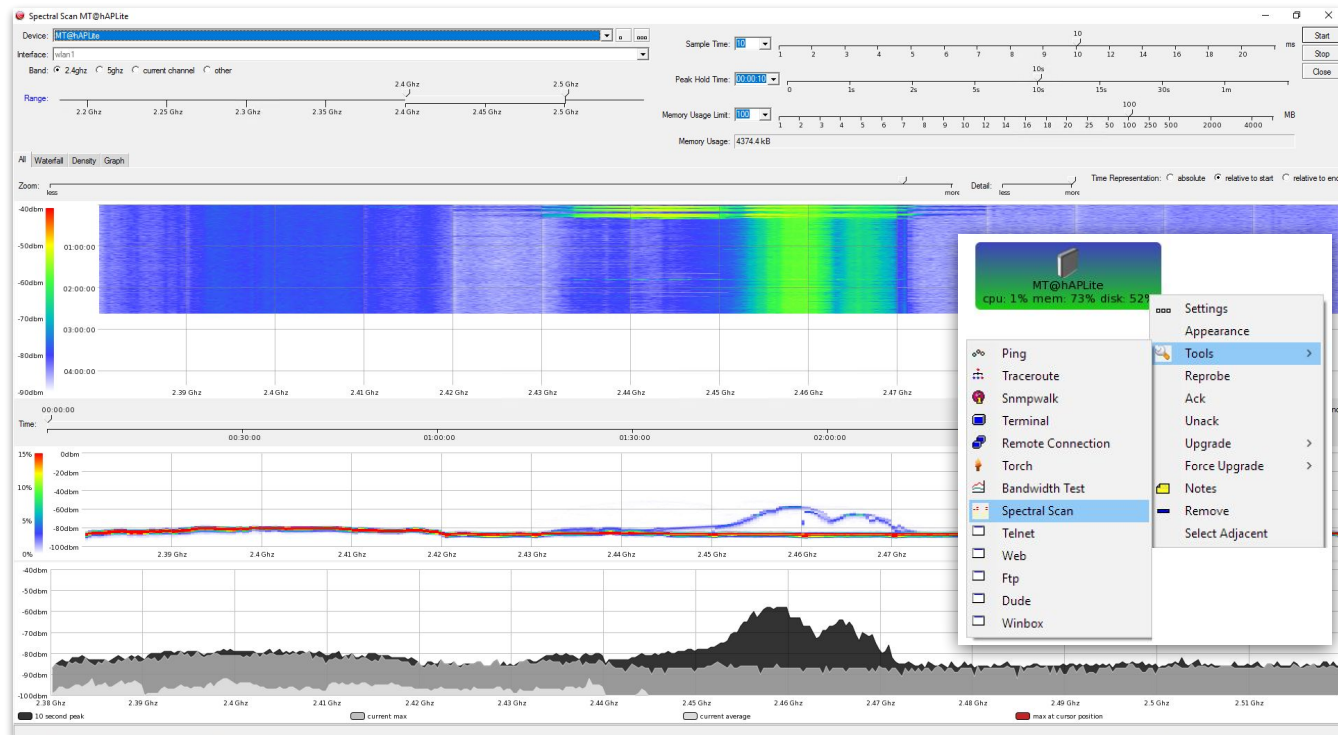
The bottom section shows the 'Access List' configuration. It includes a table with columns: #, MAC Address, MAC Mask, Interface, SSID Regexp, Signal Ra..., Action, Client To Cle..., and VLAN Mo... The table contains 6 items, with the first two rows (0 and 1) highlighted by a red box:

#	MAC Address	MAC Mask	Interface	SSID Regexp	Signal Ra...	Action	Client To Cle...	VLAN Mo...
0	90:21:...			W1		accept		
1	90:21:...					reject		
2	00:18:...			Staff		accept		
3	00:18:...					reject		
4	54:EF:...			W1_Hotspot		accept		
5	54:EF:...					reject		

Spectral scan

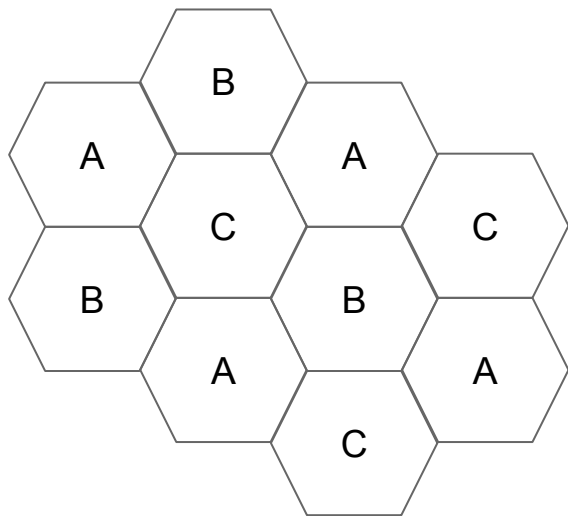
Инструментарий:
Spectral scan(The Dude)
spectral-history
spectral-scan

и много другое...



Channels

Построение сотовой сети



CAPsMAN

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

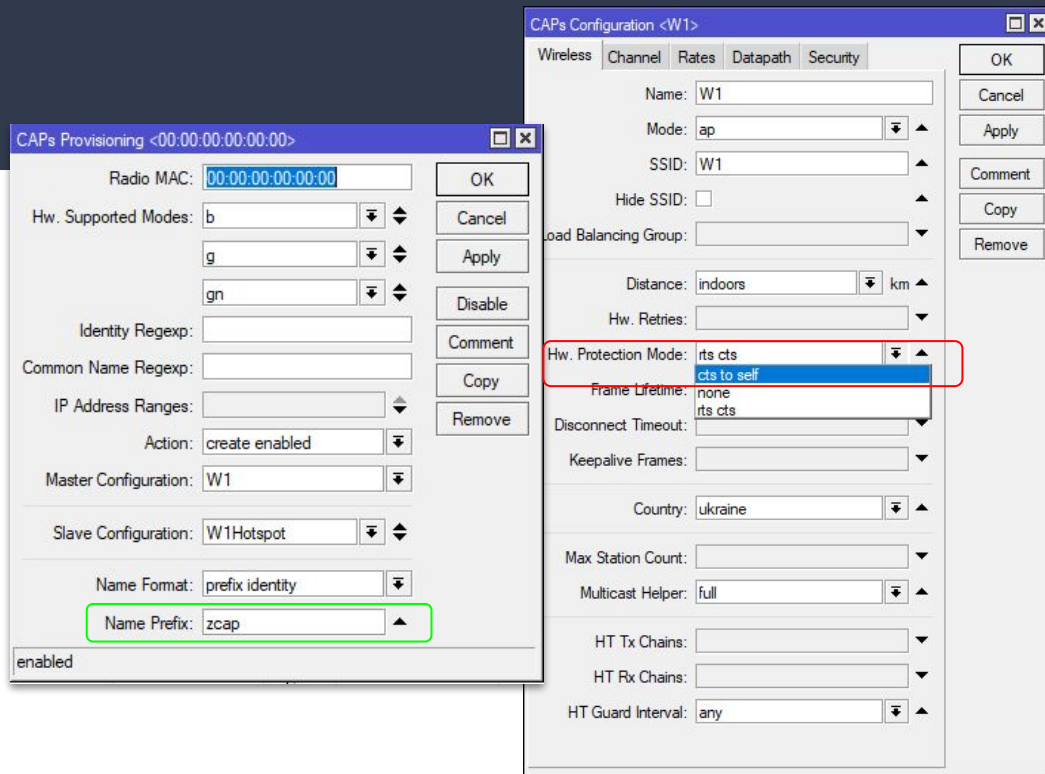
+ - [Icon] [Icon] Find

Name	Frequency	Control Channel ...	Band	Extension Channel	Tx Power
::Default	2412, 2437, 2462		2ghz-b/g/n		
::Default-greenfield(n)	2412, 2437, 2462		2ghz-onlyn		20
Group2-A	2412		2ghz-b/g/n		17
Group2-B	2437		2ghz-b/g/n		17
Group2-C	2462		2ghz-b/g/n		17
channel5.2Gh	5200		5ghz-a/n/ac		

6 items

Практические советы

- Используйте bugfix ветку.
- Оборудование Tile
- Стоит следить за актуальность версий пакетов.
- Забудьте о Fast Ethernet
- Мухи | Котлеты. ROS253 как канал для работы CAPsMAN.
- Не надо так "орать". Tx Power Rate.
- syslog-ng + python



CAPsMAN

В радиосетях нет универсальных решений. Вы развертываете сеть отталкиваясь от исследования радиоэфира и требований заказчика.

???

А также темы о которых я могу рассказать много интересного после доклада:
IPsec, PublicVPN service, HTB, R&S, Firewall ip v4/v6, костыли, велосипеды...

Ресурсы

Э. Таненбаум , Д.Уэзеролл. Компьютерные сети, 5е издание.

https://wiki.mikrotik.com/wiki/Manual:Simple_CAPsMAN_setup - intro to CAPsMAN

<https://aacable.wordpress.com/2011/11/29/howto-save-mikrotik-logs-to-remote-syslog-server/> - syslog-ng

<https://mum.mikrotik.com//presentations/RU14/wifimag.pdf> - Mesh/Mesh+WDS

<https://wiki.mikrotik.com/wiki/Manual:CAPsMAN>

https://wiki.mikrotik.com/wiki/Manual:Wireless_Debug_Logs

https://wiki.mikrotik.com/wiki/Manual:Wireless_FAQ

<https://support.google.com/chrome/a/answer/7172038?hl=en> - IEEE 802.11 codes

<https://aacable.wordpress.com/2011/12/13/monitoring-network-with-the-dude-pc-x86-or-mikrotik-npk-ver/> - SNMP Monitoring

https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/cisco_wlan_design_guide.pdf