

MUM Kyiv 2018

SAPsMAN. 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 shows the CAPsMAN main interface. The menu bar at the top includes 'CAP Interface', 'Provisioning', 'Configurations', 'Channels', 'Datapaths', 'Security Cfg.', 'Access List', 'Rates', 'Remote CAP', 'Radio', and 'Registration Table'. The 'CAP Interface' menu item is highlighted with a red box. The table below lists several CAP interfaces:

Name	Type	Tx	Rx	Tx Pac...	Rx Pa...	Configuration	SSID
zcap-MT-HomeAP-1	CAP Interface	0 bps	0 bps	0	0	W1	W1
zcap-MT-HomeAP-1-1	CAP Interface	0 bps	0 bps	0	0	W1Hotspot	W1_Hotspot
zcap-MT-HomeAP-5Hz-W1	CAP Interface	0 bps	0 bps	0	0	W1	W1
zcap-MT-HomeAP-5Hz-W1-Hotspot	CAP Interface	0 bps	0 bps	0	0	W1Hotspot	W1_Hotspot
zcap-MT-SlaveAP-1	CAP Interface	0 bps	0 bps	0	0	W1	W1
zcap-MT-SlaveAP-1-1	CAP Interface	0 bps	0 bps	0	0	W1Hotspot	W1_Hotspot

The CAPs Manager configuration dialog box is shown. The 'Enabled' checkbox is checked and highlighted with a red box. Other fields include Certificate, CA Certificate, Require Peer Certificate, Generated Certificate, Generated CA Certificate, Package Path, and Upgrade Policy.

The CAP configuration dialog box is shown. The 'Enabled' checkbox is checked and highlighted with a red box. The 'Discovery Interfaces' dropdown menu is set to 'vlan1-ros253-in' and is also highlighted with a red box. Other fields include Interfaces, Certificate, Lock To CAPsMAN, CAPsMAN Addresses, CAPsMAN Names, CAPsMAN Certificate Common Names, Bridge, Static Virtual, Requested Certificate, and Locked CAPsMAN Common Name.

Datapath

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

Wireless Tables

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

#	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

Requested

Locked CAPsMAN Co

Request CAPs Datapath Configuration <W1>

Name: W1

MTU:

L2 MTU:

ARP:

Bridge: bridge-hgw

Bridge Cost:

Bridge Horizon:

Local Forwarding:

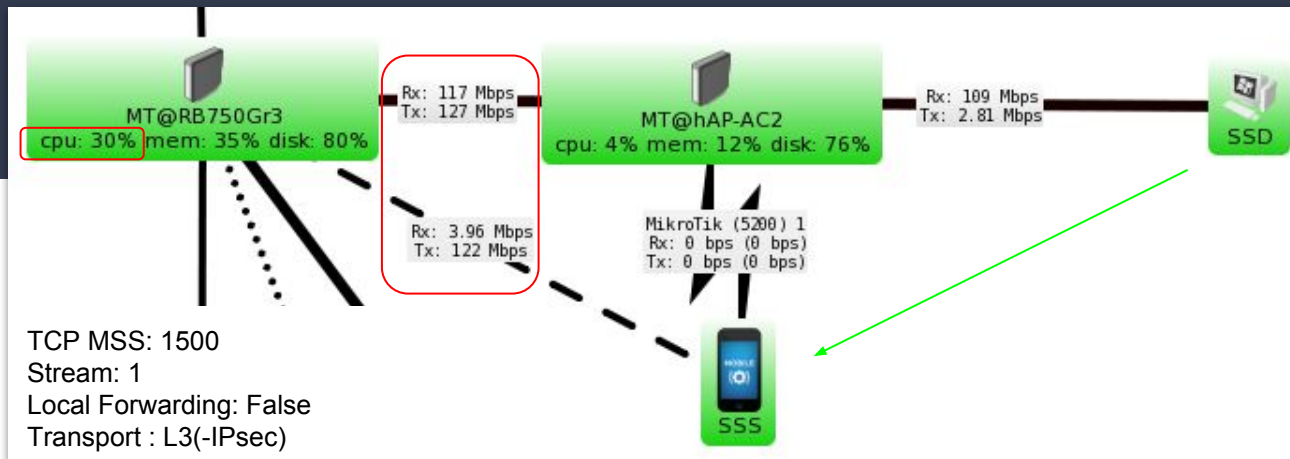
Client To Client Forwarding:

VLAN Mode:

VLAN ID:

Interface List:

Datapath



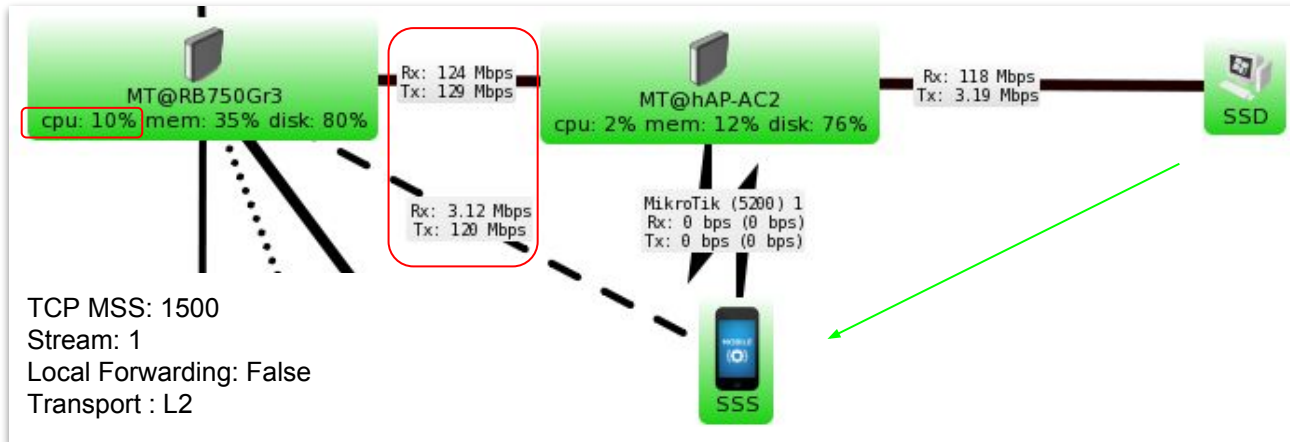
Хосты SSD и SSS входят в одноранговую сеть и находятся в L2 broadcast domain.

Нет плюсов/минусов. Есть особенности применения.

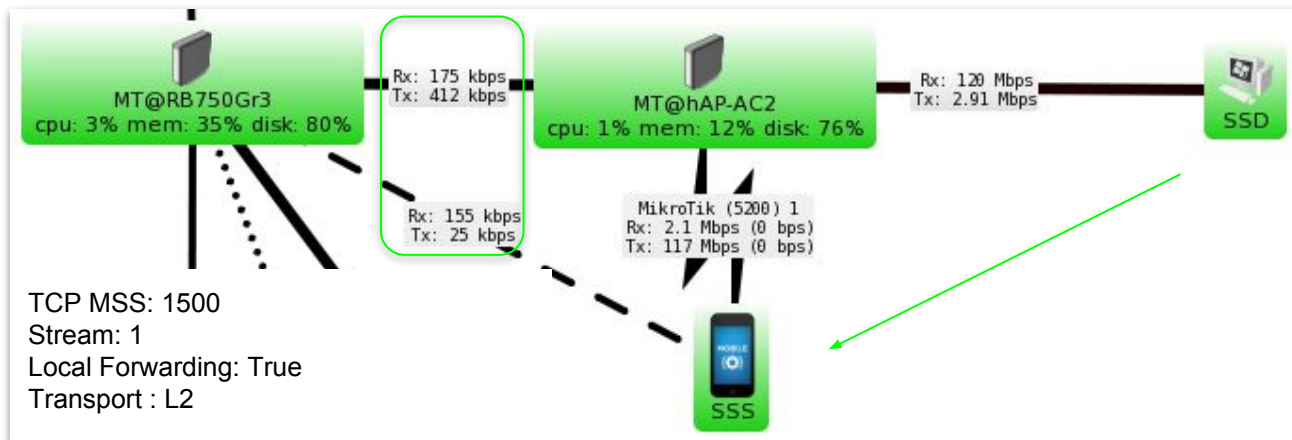
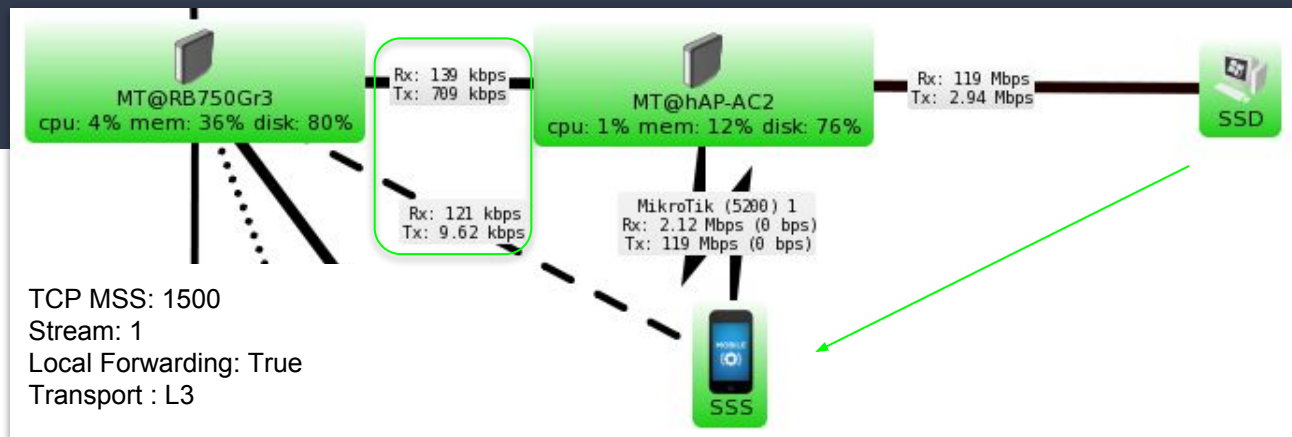
CAPsMAN не provision server.
Учитывая вышесказанное настойчиво рекомендую использовать CAPsMAN в пределах L2 broadcast domain

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

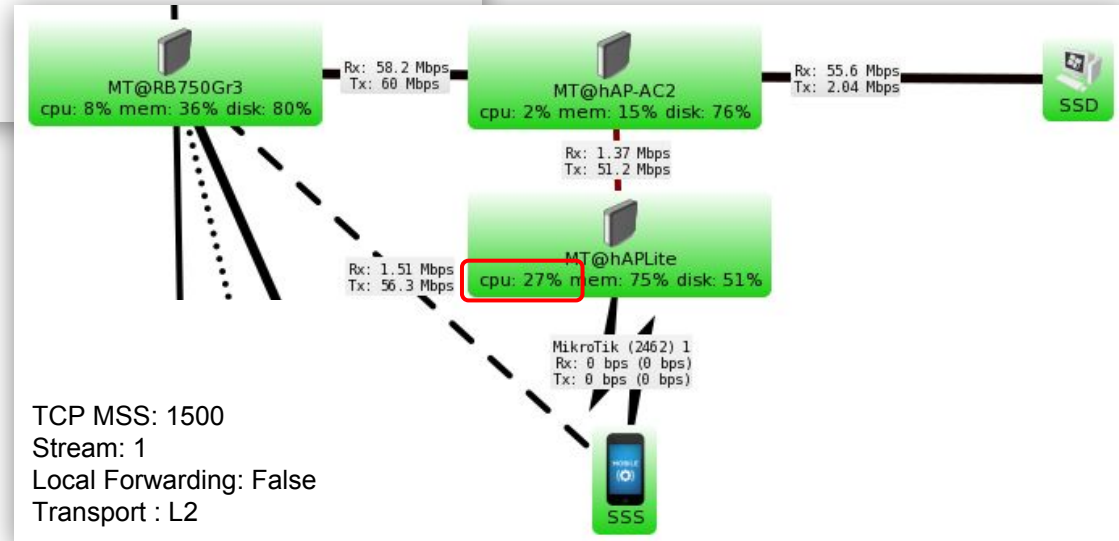
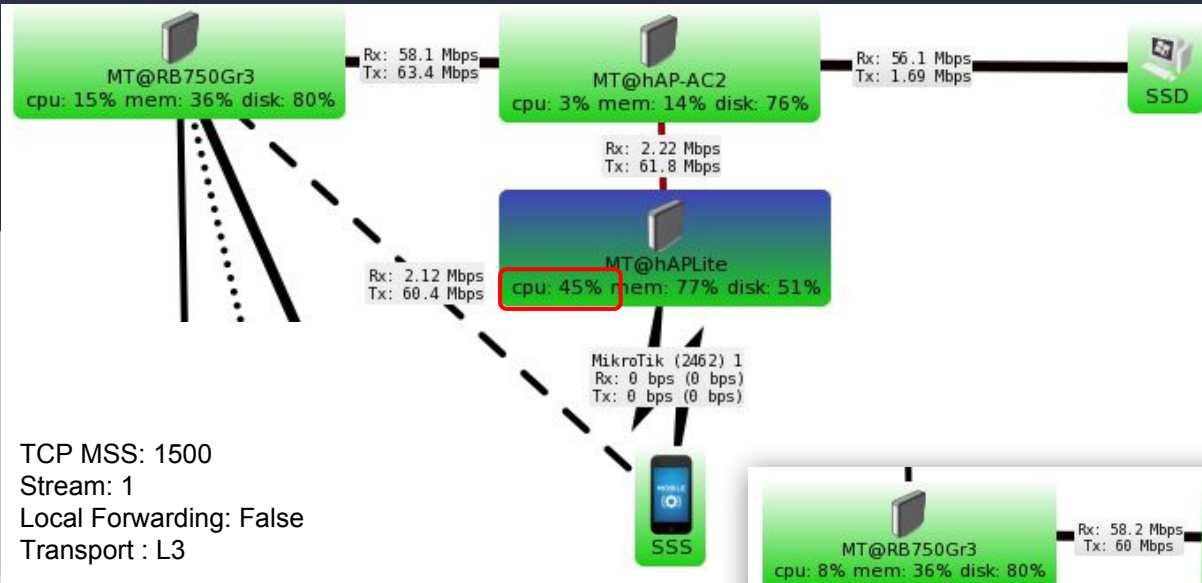
Можно не “тянуть” vlan`ы на все CAP`ы, и при необходимости натянуть IPsec(trans) при использовании IP транспорта.



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. A 'CAPs Scanner' button is visible below the navigation. The main content area shows a table with columns: Interface, SSID, MAC Address, EAP Identity, Tx Rate, and Rx Rate. The selected row is 'zcap-MT-SlaveAP-1' with Tx Rate '1Mbps' and Rx Rate '65Mbps-20MHz/1S'. A context menu is open over the table, listing 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 smaller table shows signal strength 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

Below this, it indicates '1 item (1 selected)'. The bottom part of the screenshot shows the 'Access List' configuration table with columns: #, MAC Address, MAC Mask, Interface, SSID Regexp, Signal Ra..., Action, Client To Cle..., and VLAN Mo... VL. The table contains 6 entries:

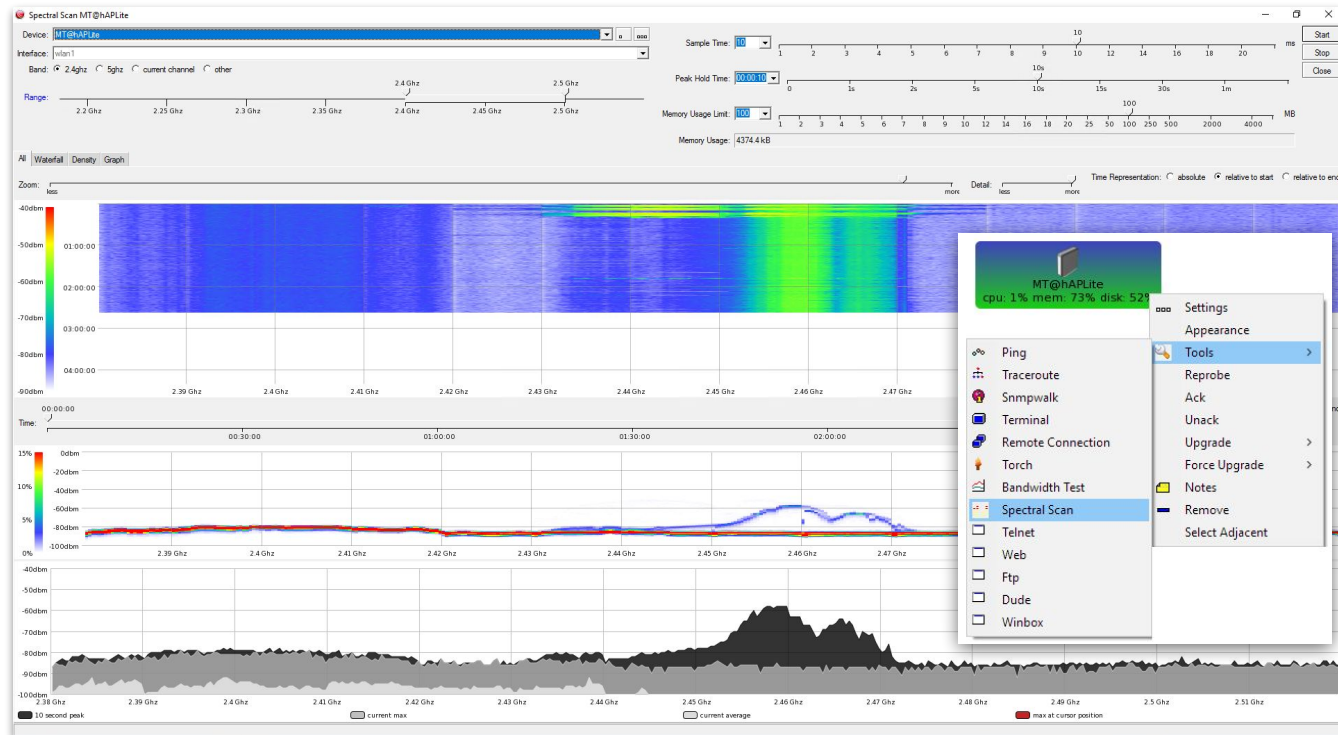
#	MAC Address	MAC Mask	Interface	SSID Regexp	Signal Ra...	Action	Client To Cle...	VLAN Mo... VL
0	90:21			W1		accept		
1	90:21					reject		
2	00:18			Staff		accept		
3	00:18					reject		
4	54:EF			W1_Hotspot		accept		
5	54:EF					reject		

The status bar at the bottom indicates '6 items'.

Spectral scan

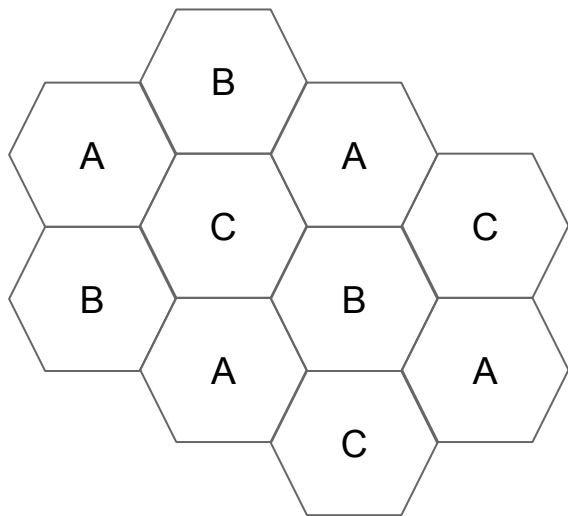
Инструментарий:
Spectral scan(The Dude)
spectral-history
spectral-scan

и много другое...



Channels

Построение сотовой сети



CAPsMAN

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

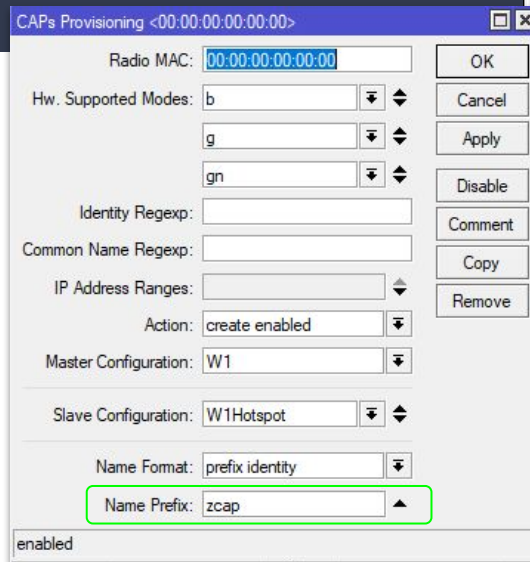
+ - [] [] Find

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



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

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

Hw. Supported Modes: b, g, gn

Identity Regexp:

Common Name Regexp:

IP Address Ranges:

Action: create enabled

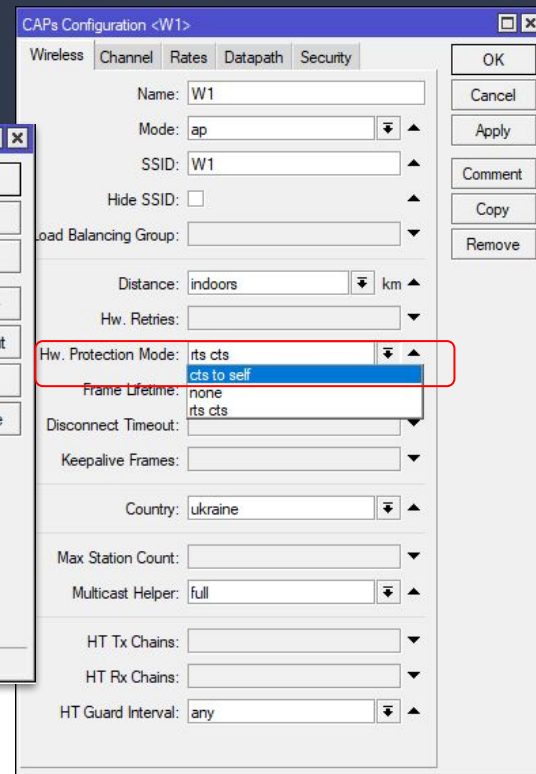
Master Configuration: W1

Slave Configuration: W1Hotspot

Name Format: prefix identity

Name Prefix: zcap

enabled



CAPs Configuration <W1>

Wireless Channel Rates Datapath Security

Name: W1

Mode: ap

SSID: W1

Hide SSID:

Load Balancing Group:

Distance: indoors km

Hw. Retries:

Hw. Protection Mode: rts cts, cts to self

Frame Lifetime: none, rts cts

Disconnect Timeout:

Keepalive Frames:

Country: ukraine

Max Station Count:

Multicast Helper: full

HT Tx Chains:

HT Rx Chains:

HT Guard Interval: any

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