MUM Kyiv 2018

CAPsMAN. Практическая реализация и неочевидные особенности.

Шишко Александр
shaman-mail@ukr.net
LinkedIn Profile

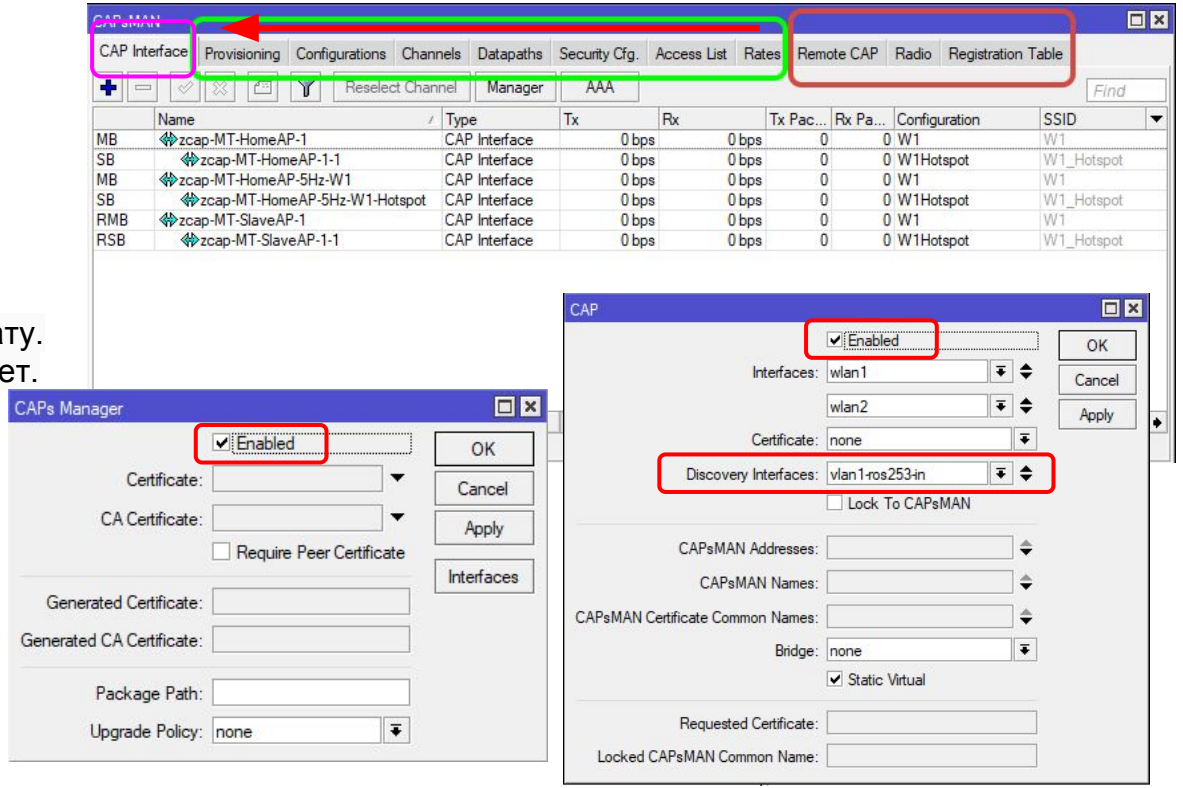
CAPsMAN

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

Беглый обзор интерфейса CAPsMAN

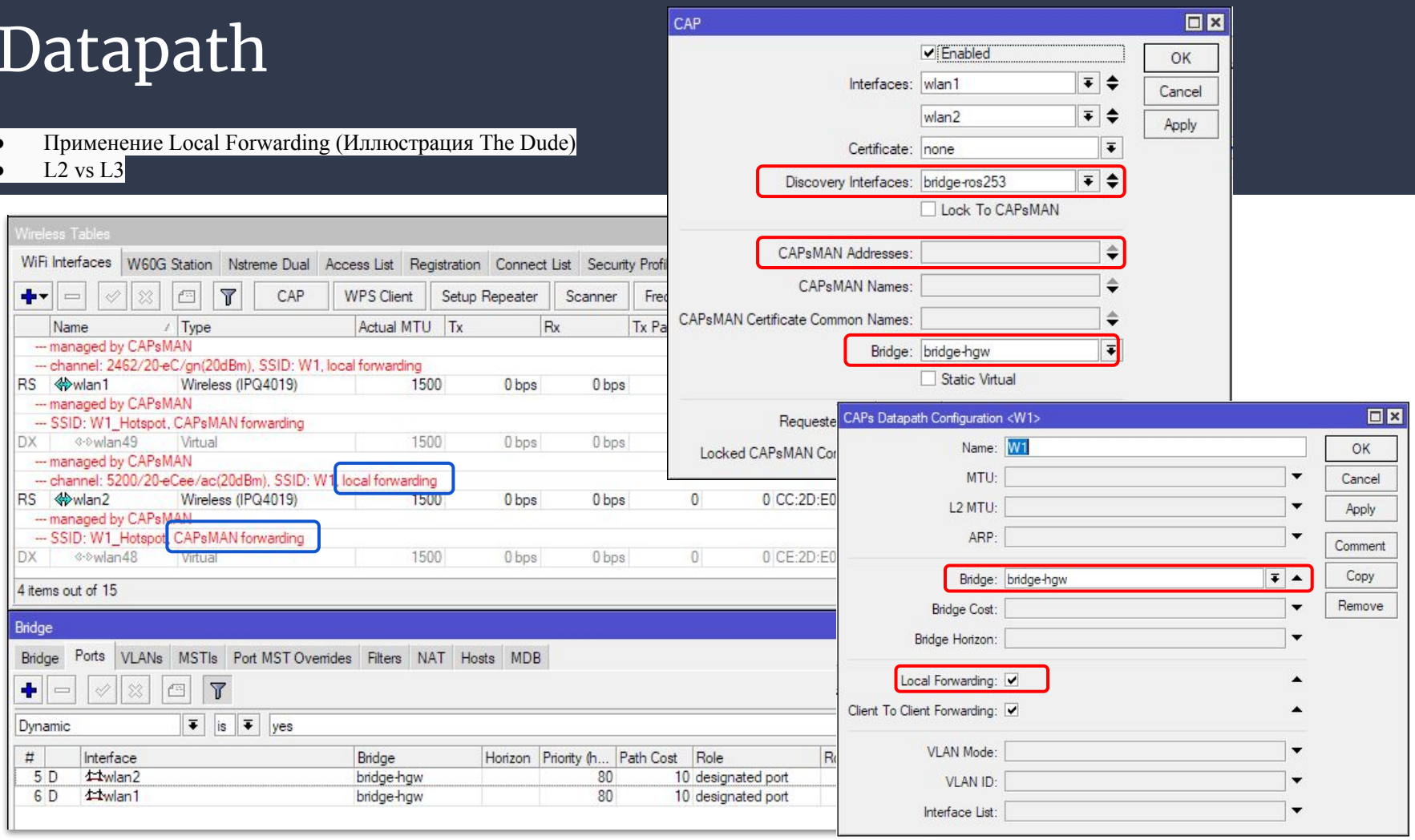
Интерфейс логически делится на 3 части:
Interfaces - Configuration - Info
Настраивается с конца.
Если не заработало:
Включить контроллер кн. Manager -> Enabled
Discovery-interfaces

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

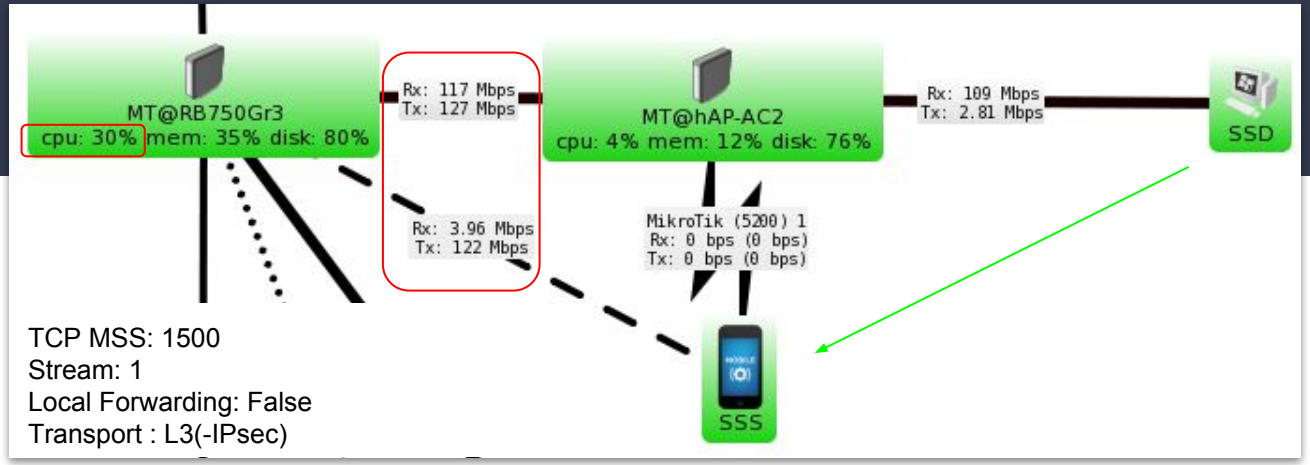


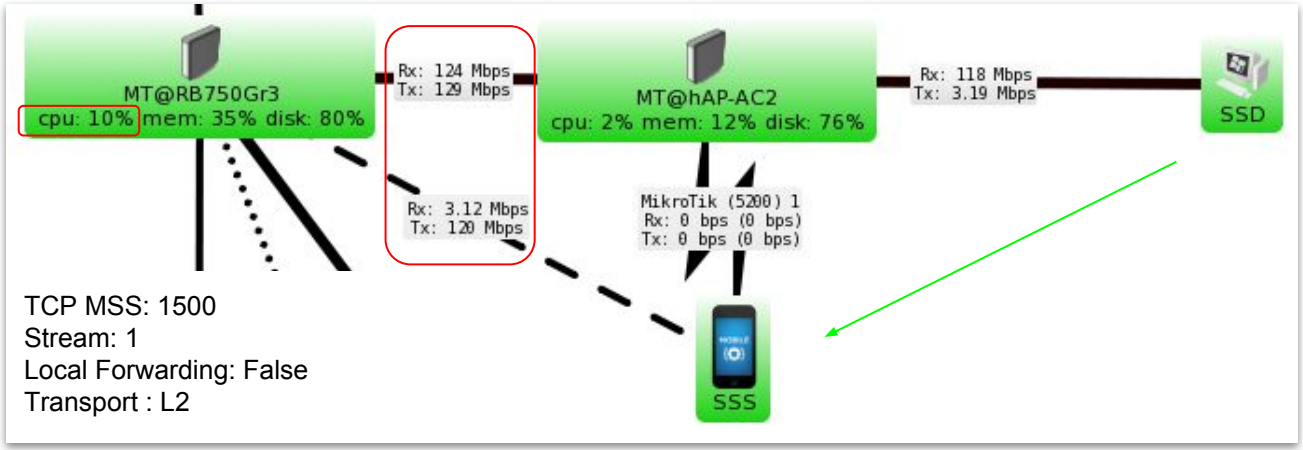
Datapath

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



Datapath





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

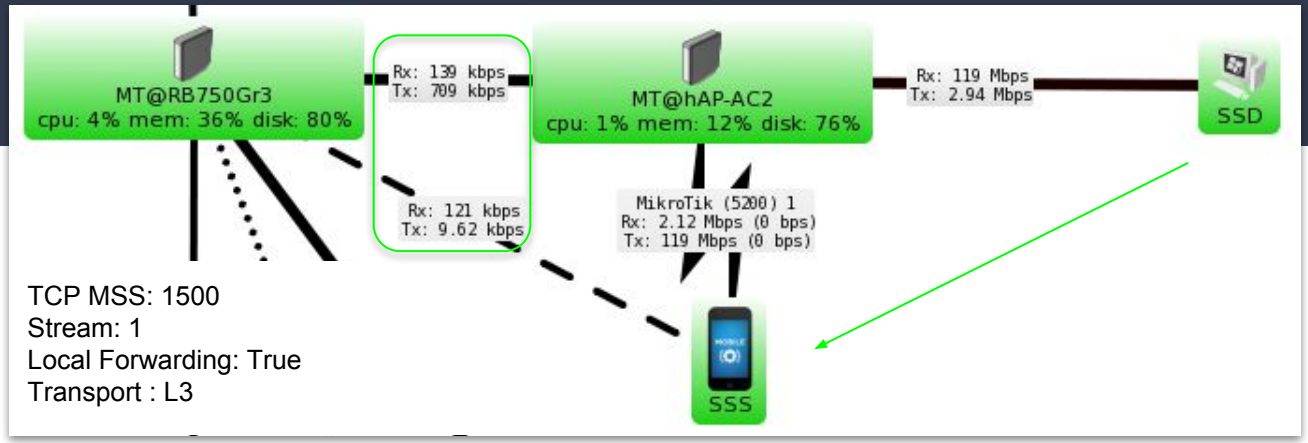
Нет плюсов/минусов. Есть особенности применения.

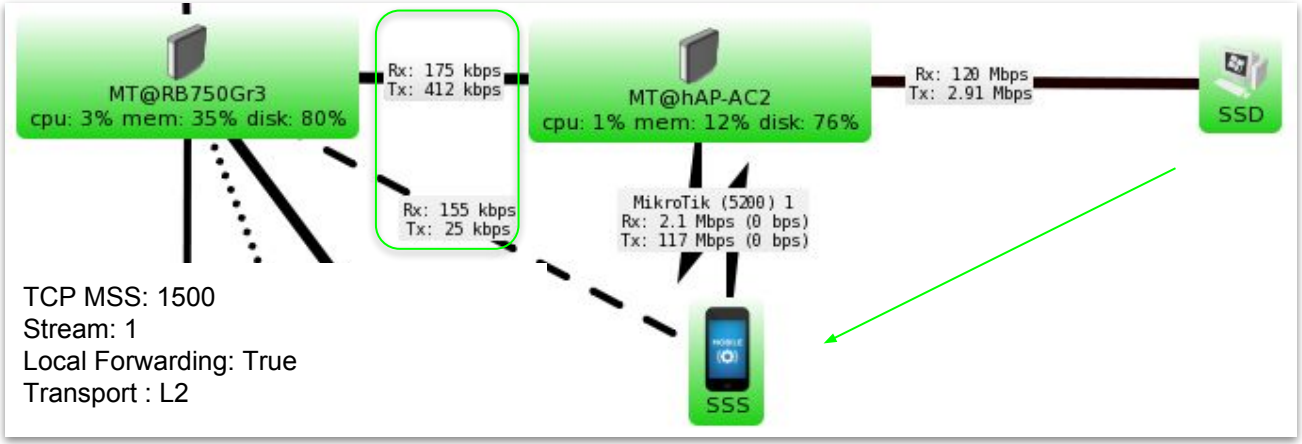
CAPsMAN не provision server. Учитывая вышесказанное настойчиво рекомендую использовать CAPsMAN в пределах L2 broadcast domain

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

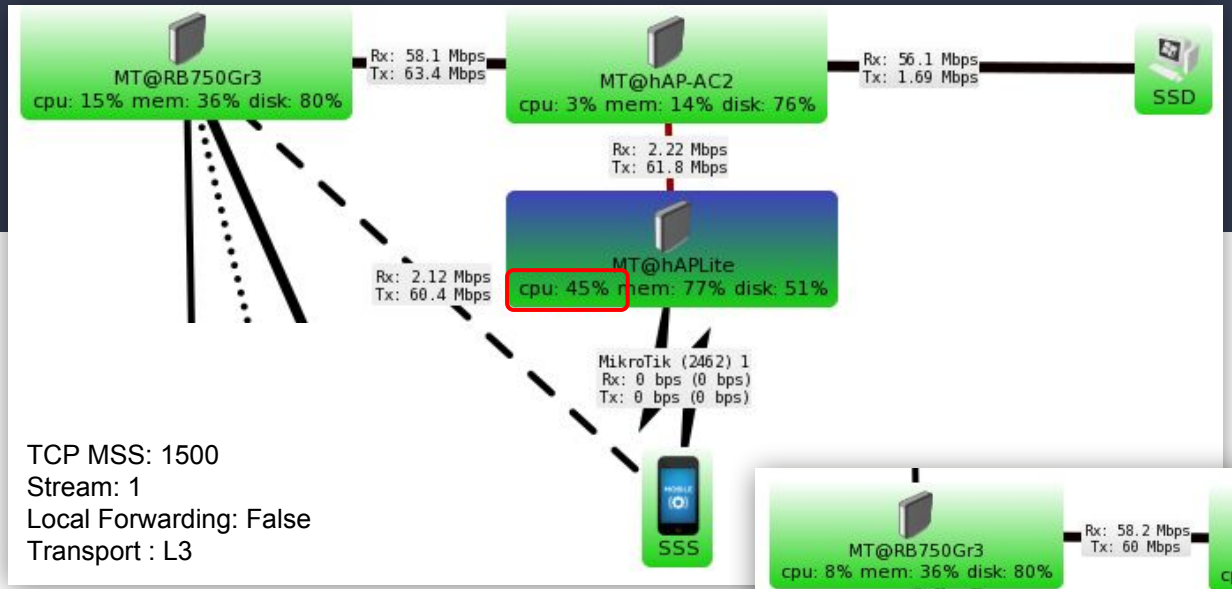
Можно не “тянуть” vlan`ы на все CAP`ы, и при необходимости натянуть IPsec(trans) при использовании IP транспорта.

Datapath

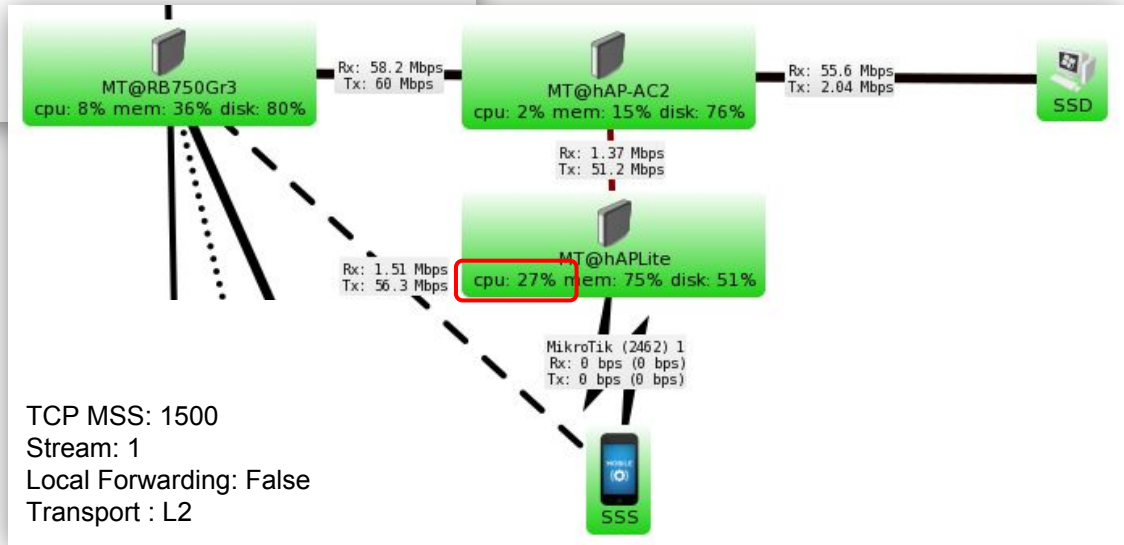

MT@RB750Gr3
cpu: 4% mem: 36% disk: 80%
Rx: 139 kbps
Tx: 709 kbps
Rx: 121 kbps
Tx: 9.62 kbps
MT@hAP-AC2
cpu: 1% mem: 12% disk: 76%
Rx: 119 Mbps
Tx: 2.94 Mbps
SSD
MikroTik (5200) 1
Rx: 2.12 Mbps (0 bps)
Tx: 119 Mbps (0 bps)
SSS
TCP MSS: 1500
Stream: 1
Local Forwarding: True
Transport : L3


MT@RB750Gr3
cpu: 3% mem: 35% disk: 80%
Rx: 175 kbps
Tx: 412 kbps
Rx: 155 kbps
Tx: 25 kbps
MT@hAP-AC2
cpu: 1% mem: 12% disk: 76%
Rx: 120 Mbps
Tx: 2.91 Mbps
SSD
MikroTik (5200) 1
Rx: 2.1 Mbps (0 bps)
Tx: 117 Mbps (0 bps)
SSS
TCP MSS: 1500
Stream: 1
Local Forwarding: True
Transport : L2

Datapath



TCP MSS: 1500
Stream: 1
Local Forwarding: False
Transport : L3



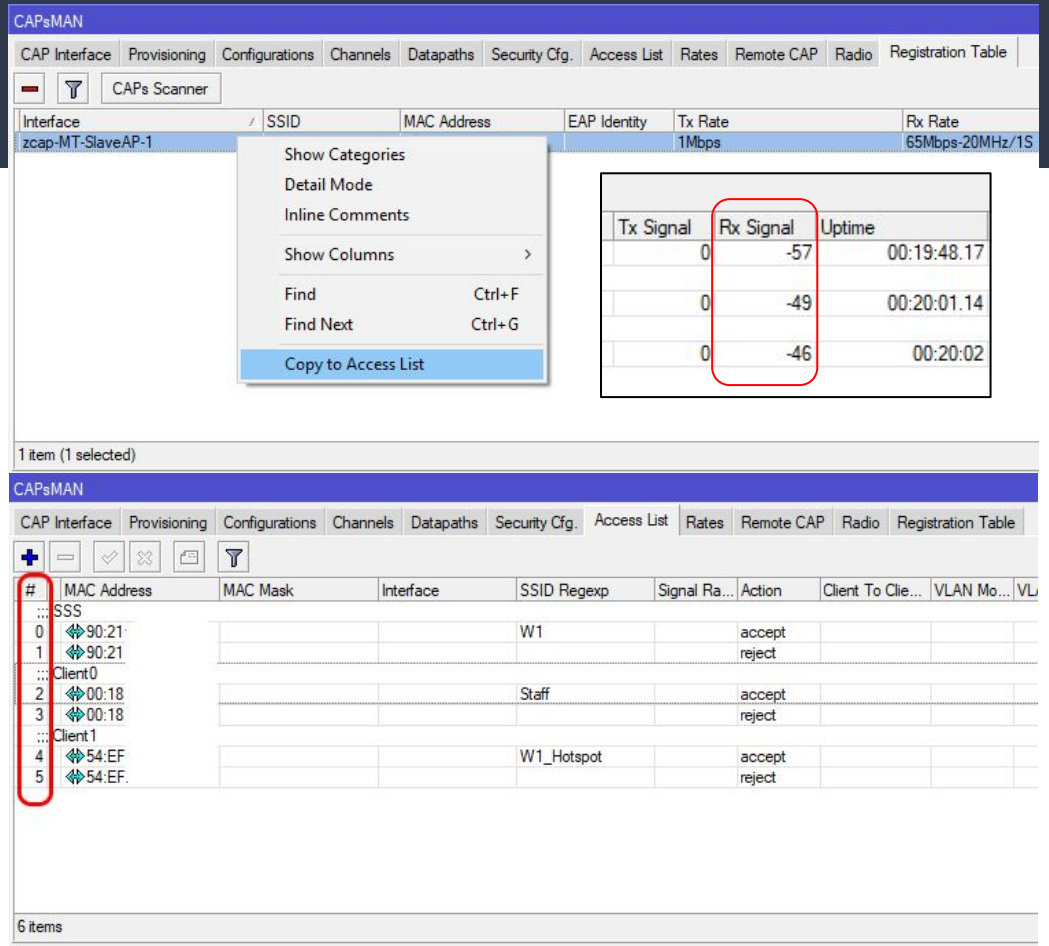
TCP MSS: 1500
Stream: 1
Local Forwarding: False
Transport : L2

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

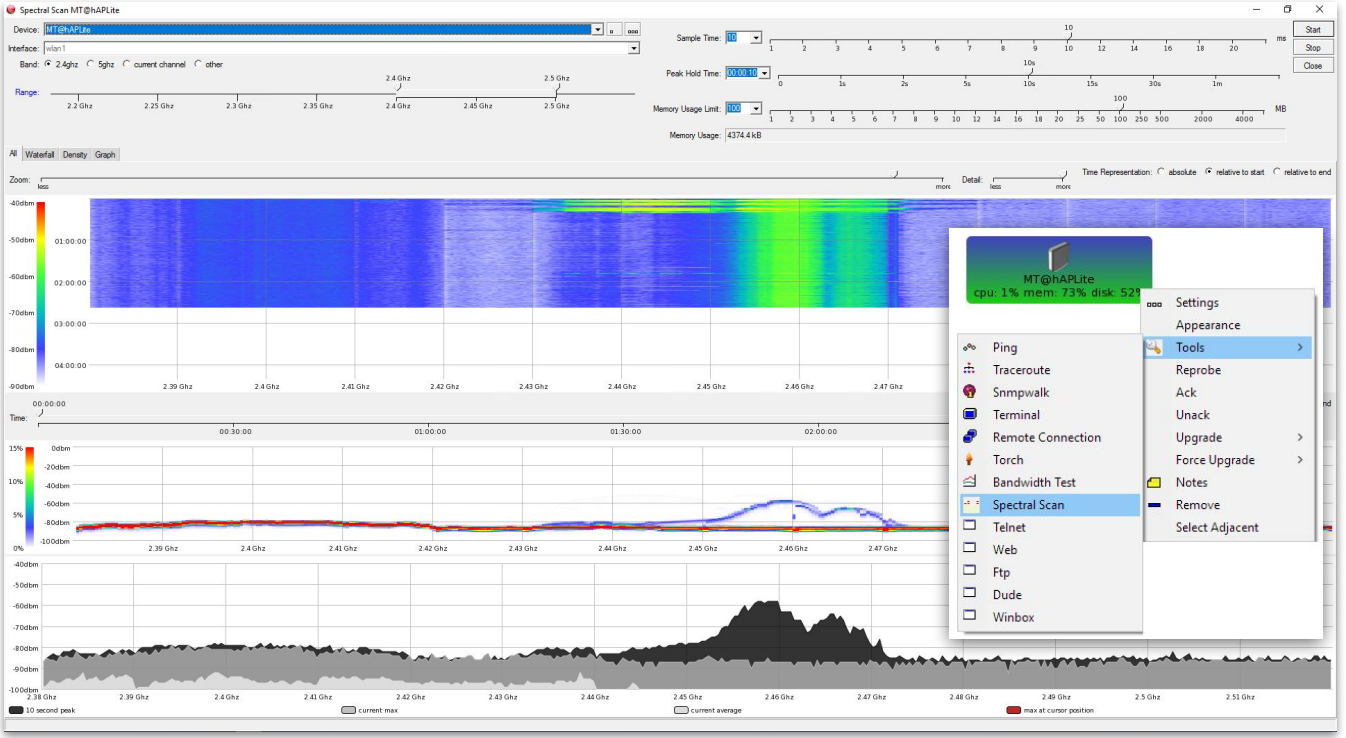
- Клиент сам выбирает где ему хорошо.
- Особенности реализации клиентских устройств.
- ACL - Конвейер
- Комментарии в ACL -> Reg. Table
- "Бесшовный роуминг" и CAPsMAN.
  О Mesh + WDS поговорим в другой раз.
  Ссылка в конце.



Spectral scan

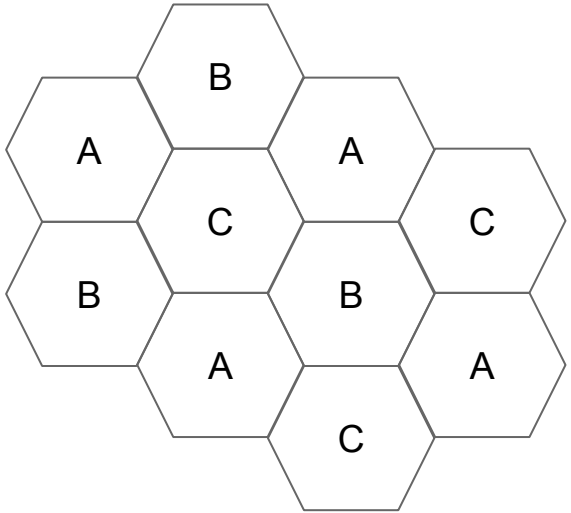
Инструментарий:
Spectral scan(The Dude)
spectral-history
spectral-scan

и много другое...



Channels

Построение сотовой сети



CAPsMAN

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

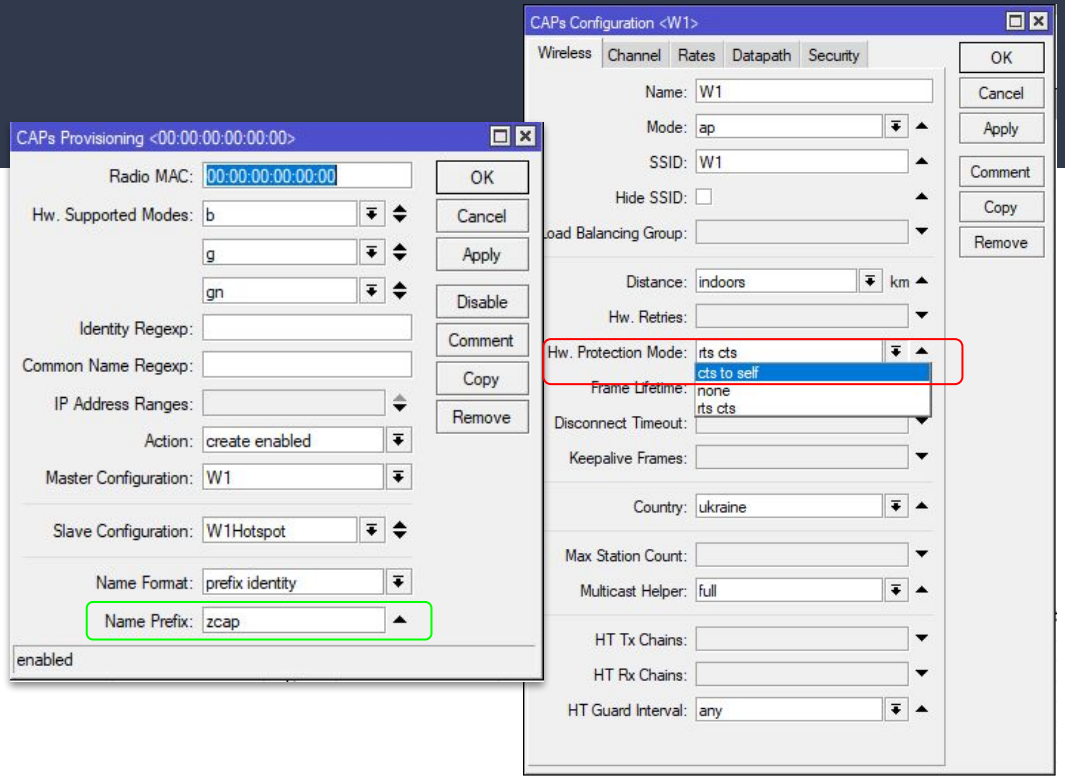
Find

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



CAPsMAN

В радиосетях нет универсальных решений. Вы развертываете сеть отталкиваясь от иследования 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