

CAPsMAN на RouterOS 7: Как организовать централизованное управление Wi-Fi

Спикер:
Роман Козлов

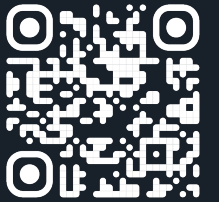


ЗА 1-е МЕСТО В ВИКТОРИНЕ

Худи от Вокс Линк

Спонсор подарка

voxlink



- Интегратор IP телефонии на базе Asterisk для вашего бизнеса
- На рынке с 2011 года, 1600+ проектов
- Наш дистрибутив VoxDistro входит в реестр Российского ПО



ПОДАРКИ ОТ
СПОНСОРОВ



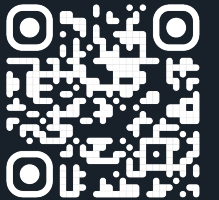
ЗА 2-е МЕСТО В ВИКТОРИНЕ

Футболка

“Смерть мерзкая от микротиков”
от Вокс Линк

Спонсор подарка

voxlink



- Наш продукт CallForce - решение для колл-центров
- IP-телефония для крупного и среднего бизнеса



ПОДАРКИ ОТ
СПОНСОРОВ

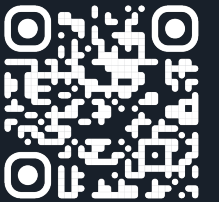
СМЕРТЬ
МЕРЗКАЯ
ОТ
МИКРОТИКОВ
ГРОБ ГРОБ КЛАДБИЩЕ ПОСЕР

ПОЛУЧИТ САМЫЙ
ВЕЗУЧИЙ ИЗ
УЧАСТНИКОВ,
ПРИШЕДШИХ ОЧНО

Кружка, сумка, ручка,
блокнот от Вокс Линк

Спонсор подарка

voxlink

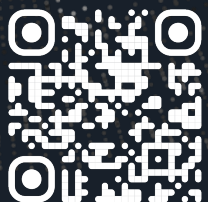


- Модернизация IP-АТС
- Переход на телефонию независимую от санкций
- Безопасность телефонии от нелегальных звонков



Орг вопросы:

Будет ли запись -
запись будет!



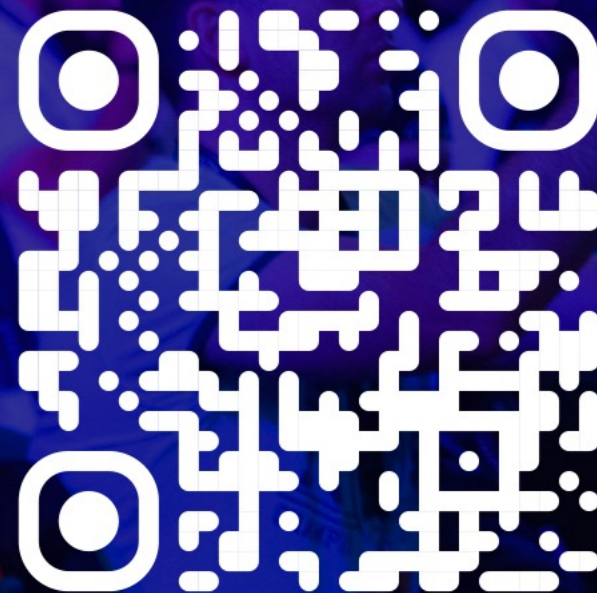


18 сентября 2024

Москва, Ярославское ш., 124
Участие очное и онлайн

Оставляйте заявку
на билет

MIKROTİK **USER** **MEETING**
mum
RUSSIA



► План

- Что такое CAPsMAN
- Создание конфигурации
- Настройка CAP
- Особенности

Что такое CAPsMAN

▶ CAPsMAN

01

Система управления точками доступа MikroTik, которая позволяет централизованно управлять настройками WIFI интерфейсов. Это WIFI контроллер

02

Также позволяет контролировать доступ клиентов на точки доступа.

03

На текущий момент актуальны две версии:

Для устройств поддерживающих пакет wifi-qcom / wifi-qcom-ac и для устройств на пакете wireless

► WifiWave2 (7.12 and older)

- WPA3 authentication and OWE (opportunistic wireless encryption)
- 802.11r/k/v
- MU-MIMO and beamforming
- 400Mb/s maximum data rate in the 2.4GHz band for IPQ4019 interfaces
- OFDMA

► Оборудование


пакет wifi-qcom

- Hap ax2
- Hap ax3
- Chateau ax
- CAP ax
- Hap ax lite
- L009UiGS-2HaxD-IN
- L11UG-5HaxD
- L23UGSR-5HaxD2HaxD

Пакет wifi-qcom-ac

- Hap ac2
- Hap ac3
- Chateau
- Audience
- RB4011iGS+5HacQ2HnD-IN
- CAP XL ac
- CAP ac
- Wap ac (arm)

Package List





Check For Updates


Enable

Disable

Uninstall

Name	Version	Build Time
 routeros	7.16beta4	Jul/02/2024 12:47:41
 wifi-qcom	7.16beta4	Jul/02/2024 12:47:41

Package List





Check For Updates

Enable

Disable

Uninstall

Name	Version	Build Time
 routeros	7.16beta4	Jul/02/2024 12:47:41
 wifi-qcom-ac	7.16beta4	Jul/02/2024 12:47:41

Создание конфигурации

► WifiWave2 CAPsMAN

- Находится в разделе WiFi
- Активируется в разделе remote CAP
- `/interface/wifi/capsman/set enabled=yes`
- Требуется собирать конфигурации под разные задачи
- Конфигурацию можно собирать в разделе `/interface/wifi/configuration` или в соответствующих разделах
- Локальные интерфейсы не настраиваются в capsman, а используются с local manager
- На сар устройствах не требуется настраивать конфигурацию

The screenshot shows the Mikrotik WinBox interface for configuring CAPsMAN. The main window has tabs for 'WIFI', 'Configuration', 'Channel', 'Security', 'AAA', 'Datapath', 'Interworking', 'Steering', 'Registration', 'Access List', 'Provisioning', 'Radios', and 'Remote CAP'. The 'WIFI' tab is active, and the 'CAPsMAN' sub-tab is selected. Below the tabs, there are fields for 'Address', 'Identity', 'Board', 'Serial', and 'Version'. A 'CAPsMAN' dialog box is open, showing the following options:

- ☐ Enabled
- Interfaces: [dropdown menu]
- CA Certificate: [dropdown menu]
- Certificate: [dropdown menu]
- ☐ Require Peer Certificate
- Package Path: [text field]
- Upgrade Policy: [dropdown menu, currently set to 'none']
- Generated CA Certificate: [text field]
- Generated Certificate: [text field]

Buttons for 'OK', 'Cancel', and 'Apply' are located on the right side of the dialog box.

► WifiWave2 Security

- Режим совместимости (WPA2/WPA3) работает достаточно странно
- Для WPA3 обязательна настройка защиты служебных кадров 802.11w (management protection)
- Поддержка аппаратных особенностей устройства можно посмотреть в разделе radios
- Раздел EAP – настройки опций при использования radius
- FT – Fast Transition настройки необходимые для 802.11r (могут быть добавлены или переопределены в configurations)

WiFi Security <sec1>

Security EAP FT

Name: sec1

Authentication Types

Types: ☐ WPA PSK ☐ WPA2 PSK ☐ WPA EAP ☐ WPA2 EAP
☒ WPA3 PSK ☐ OWE ☐ WPA3 EAP ☐ WPA3 EAP 192

Encryption

Group Encryption: GCMP 256

Group Key Update:

Passphrase: *****

Disable PMKID:

Management Protection: required

Management Encryption: GMAC 256

WPS:

DH Groups:

SAE Anti Clogging Threshold:

SAE Max Failure Rate:

SAE PWE:

OWE Transition Interface:

Connect Group:

Connect Priority:

enabled

OK Cancel Apply Disable Comment Copy Remove

► WifiWave2 Security FT

The screenshot shows the Mikrotik WinBox interface. At the top, there's a menu bar with tabs: WiFi, Configuration, Channel, Security, AAA, Datapath, Interworking, Steering, Registration, Access List, Provisioning, Radios, and Remote CA. Below the menu bar is a toolbar with icons for adding, deleting, and editing configurations. The main window displays a table with columns: Name, Types, Ciphers, Group Encryption, and Passphrase. A modal window titled 'WiFi Security <sec1-corp>' is open, showing the 'Security' tab. Inside this tab, there are sub-tabs for 'Security', 'EAP', and 'FT'. The 'FT' sub-tab is active, showing the 'FT Enabled' checkbox checked, 'FT Mobility Domain' set to '1', and several other fields like 'FT Over DS', 'FT Reassoc. Deadline', 'FT NAS Identifier', 'FT RO Key Lifetime', and 'FT Preserve VLAN ID'. On the right side of the modal window, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'.

- Fast BSS Transition работает с сетями WPA-EAP2/3, WPA2/3 и полностью открытыми сетями. Для WPA2/3-PSK теряется смысл быстрого роуминга, т.к. клиент и точка всё равно обмениваются 4 пакетами, ускорять тут нечего.
- FT Mobility Domain - необходим для успешного роуминга, который возможен только в пределах одного домена
- При использовании radius необходимая настройка для быстрого перехода
- Клиенты не поддерживающие 802.11r не смогут подключиться к данной сети

► WifiWave2 Cannel

WiFi

WiFiConfigurationChannelSecurityAAADatapathInterworkingSteeringRegistrationAccess ListProvisioningRadiosRemote CAP

Name	Band	Channel ...	Frequency
channel_5Ghz_AC	5GHz AC	20MHz	5180, 5200, 5220, 5240, 5260, 5280, 5300, 5320, 5500, 5520, 5540, 5560, 5580, 5600, 5620, 5640, 5660, 5680, 5700, 5720, 5745, 5765, 5785, 5805, 5825
channel_5Ghz_AC_bc	5GHz AC	20MHz	5180, 5200, 5220, 5240
channel_5Ghz_AX	5GHz AX	20MHz	5180, 5200, 5220, 5240, 5260, 5280, 5300, 5320, 5500, 5520, 5540, 5560, 5580, 5600, 5620, 5640, 5660, 5680, 5700, 5720, 5745, 5765, 5785, 5805, 5825
channel_5Ghz_AX_bc	5GHz AX	20MHz	5180, 5200, 5220, 5240
channel_24Ghz_AX	2GHz AX	20MHz	2412, 2437, 2462, 2472
channel_24Ghz_N	2GHz N	20MHz	2412, 2437, 2462, 2472

- Настройка каналов и поддерживаемых технологий для точек доступа
- В 2.4Ghz диапазоне 1-6-11 (13 добавлен в качестве домашней альтернативы)
- В 5Ghz – набор наиболее лучших каналов –
 - Наиболее совместимые каналы 36,40,44,48
 - Каналы со средней совместимостью – 52,56,60,64,132,136,140,149,153,157,161,165
 - Каналы с низкой совместимостью – 100, 104,108,116,144
 - Каналы под вопросом – 112, 120, 124, 128
- Band – указываем максимальный стандарт для точки доступа, режим совместимости не отключается
- В корпоративных и 2.4Ghz сетях ширина каналов 20Mhz

► WifiWave2 Cannel

/interface wifi channel

add band=2ghz-ax disabled=no frequency=2412,2437,2462,2472 name=channel_24Ghz_AX width=20mhz

add band=5ghz-ax disabled=no

frequency=5180,5200,5220,5240,5260,5280,5300,5320,5500,5520,5540,5560,5580,5600,5620,5640,5660,5680,5700,5720,5745,5765,5785,5805,5825 name=channel_5Ghz_AX secondary-frequency=disabled width=\20mhz

add band=2ghz-n disabled=no frequency=2412,2437,2462,2472 name=channel_24Ghz_N width=20mhz

add band=5ghz-ac disabled=no

frequency=5180,5200,5220,5240,5260,5280,5300,5320,5500,5520,5540,5560,5580,5600,5620,5640,5660,5680,5700,5720,5745,5765,5785,5805,5825 name=channel_5Ghz_AC secondary-frequency=disabled width=\20mhz

add band=5ghz-ax disabled=no frequency=5180,5200,5220,5240 name=channel_5Ghz_AX_bc secondary-frequency=disabled width=20mhz

add band=5ghz-ac disabled=no frequency=5180,5200,5220,5240 name=channel_5Ghz_AC_bc secondary-frequency=disabled width=20mhz

► WifiWave2 Datapath

WIFI					
WIFI	Configuration	Channel	Security	AAA	Datapath
<div><div>+</div><div>-</div><div>✓</div><div>✗</div><div>📄</div><div>🔍</div></div>					
Name		Bridge Horizon	Client Isolation	VLAN ID	
datapath-corp-AC/N					
datapath-corp-AX				111	
datapath-guest-AC/N		10	yes		
datapath-guest-AX		10	yes	112	

- CAPsMAN WifiWave2 не поддерживает capsmen forwarding - поэтому tag VLAN должны доходить до точек доступа
- Устройства wifi-qcom-ac не поддерживают назначение VLAN через datapath
- Horizon позволяет изолировать интерфейсы внутри bridge друг от друга
- Client Isolation настройка для изоляции клиентов внутри одного интерфейса WIFI

WifiWave2 Configuration

WiFi

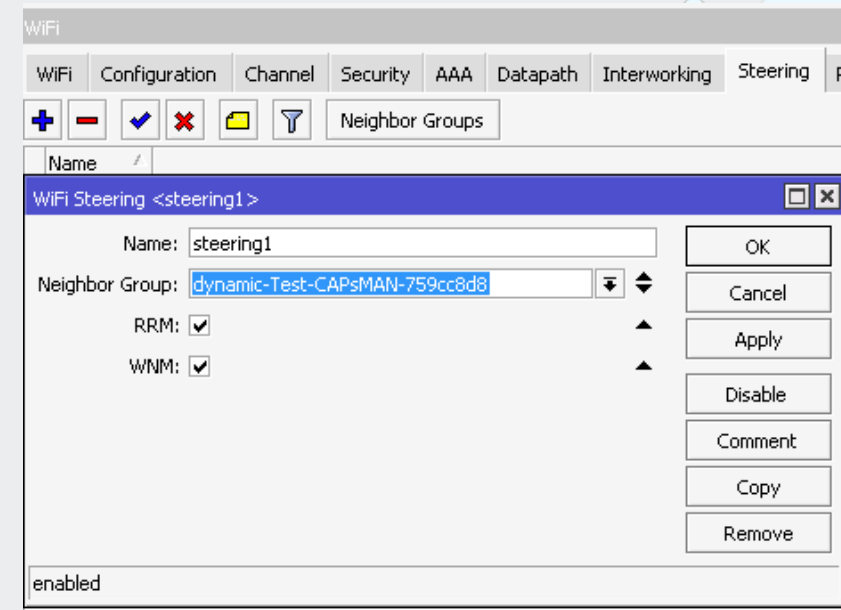
WiFi Configuration Channel Security AAA Datapath Interworking Steering Registration Access List Provisioning Radios Remote CA

Name	SSID	Channel	Security	Datapath	Steering
cfg1-5GHZ-AC	Test-CAPsMAN	channel_5Ghz_AC_bc	sec1-corp	datapath-corp-AC	steering1
cfg1-5GHZ-AX	Test-CAPsMAN	channel_5Ghz_AX_bc	sec1-corp	datapath-corp-AX	steering1
cfg1-24GHZ-AX	Test-CAPsMAN	channel_24Ghz_AX	sec1-corp	datapath-corp-AX	steering1
cfg1-24GHZ-N	Test-CAPsMAN	channel_24Ghz_N	sec1-corp	datapath-corp-AC	steering1
cfg2-Guest-AC	Test-CAPsMAN-guest		sec2-guest	datapath-guest-AC	
cfg2-Guest-AX	Test-CAPsMAN-guest		sec2-guest	datapath-guest-AX	

- CAPsMAN WifiWave2 не поддерживает capsman forwarding - поэтому tag VLAN должны доходить до точек доступа
- Устройства wifi-qcom-ac не поддерживают назначение VLAN через datapath
- Horizon позволяет изолировать интерфейсы внутри bridge друг от друга
- Client Isolation настройка для изоляции клиентов внутри одного интерфейса WIFI
- Приходится делать наборы конфигураций для разных устройств и SSID
- Гостевые конфигурации не требуют настройки каналов – будет взята конфигурация из основного интерфейса

► WifiWave2 Steering

- Управление 802.11k(RRM) и 802.11v(WNM) осуществляется через раздел steering
- Neighbor Group – группа рассылки сообщений RRM и WNM
- RRM Radio Resource Management– позволяет сообщить абонентскому устройству список соседних точек доступа, чтобы не сканировать весь доступный диапазон
- WNM Wireless Network Management - эффективное управление беспроводной средой – обмен данными о среде между станциями, энергосбережение клиента, улучшение процесса роуминга и балансировки – клиенту отправляются сообщения с подходящими AP



► WifiWave2 Provisioning

WiFi

WiFiConfigurationChannelSecurityAAADatapathInterworkingSteeringRegistrationAccess ListProvisioningRadiosRemote CAP

#	Radio MAC	Supported Bands	Action	Master Confi...	Slave Configurations	Name Format	
0		5GHz AX	create enabled	cfg1-5GHZ-AX	cfg2-Guest-AX	5AX-%I	
1		5GHz AC	create enabled	cfg1-5GHZ-AC	cfg2-Guest-AC	5AC-%I	
2		2GHz AX	create enabled	cfg1-24GHZ-AX	cfg2-Guest-AX	2AX-%I	
3		2GHz N	create enabled	cfg1-24GHZ-N	cfg2-Guest-AC	2N-%I	
4			none				

- Provisioning – правила позволяющие получать настройки на сар устройствах
- Настройки можно получать по mac адресам интересов, поддерживаемых стандартов, ip адресов или identity
- Правила работают сверху вниз

► WifiWave2 Access List

WiFi

WiFi

Configuration

Channel

Security

AAA

Datapath

Interworking

Steering

Registration

Access List

Provisioning

Radios

Remote CAP

+




-

✓

✗

📄

🔍

#	MAC Add...	MAC Add...	Interface	Signal Range	Action	
0				-75..-20	accept	
1				-120..-76	reject	
2				-19..120	reject	

- Несмотря все технологии помощников в некоторых ситуациях приходится использовать ограничения по уровню сигнала от клиента

/interface wifi access-list

add action=accept allow-signal-out-of-range=10s disabled=no signal-range=-75..-20

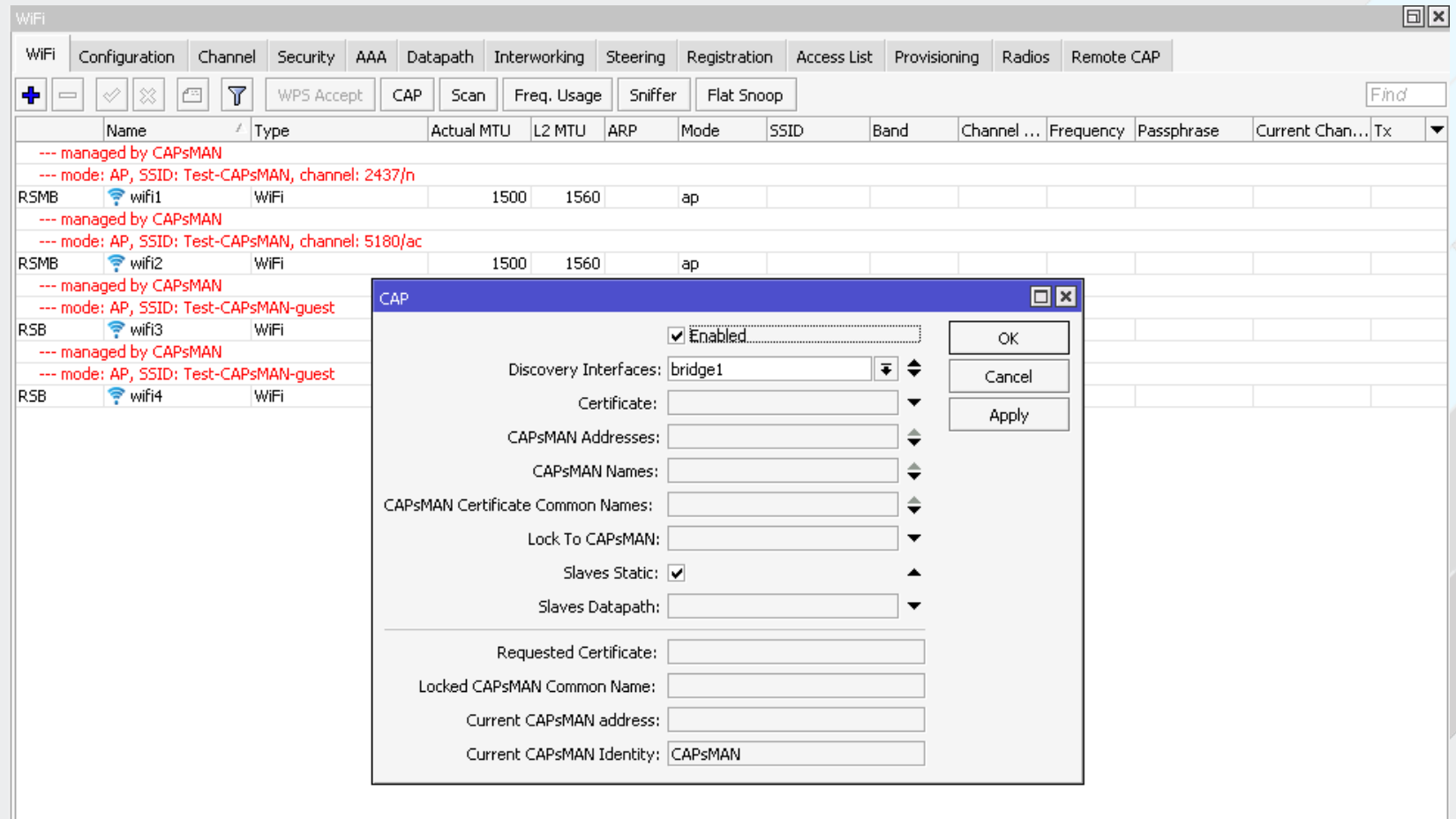
add action=reject allow-signal-out-of-range=10s disabled=no signal-range=-120..-76

add action=reject allow-signal-out-of-range=10s disabled=no signal-range=-19..120

Настройка CAP

WifiWave2 wifi-qcom-ac

- Устройства с wifi-qcom-ac не поддерживают передачу VLAN от контроллера
- Настройка должна включать назначение статических интерфейсов
- Назначение vlan происходит через bridge vlan filtering
- `/interface wifi cap set discovery-interfaces=bridge1 enabled=yes slaves-static=yes`



WifiWave2 wifi-qcom-ac bridge

Bridge									
Bridge Ports									
Port Extensions VLANs MSTIs Port MST Overrides Filters NAT Hosts MDB									
+ - ✓ ✗ [icon] [icon]									
#	Interface	Bridge	Horizon	Trusted	Priority (...)	PVID	Role	Actual Pa...	
0	ether1	bridge1		no	80	1	designated port	20000	
1	wifi1	bridge1		no	80	111	designated port	20000	
2	wifi2	bridge1		no	80	111	designated port	20000	
3	wifi3	bridge1	10	no	80	112	designated port	20000	
4	wifi4	bridge1	10	no	80	112	designated port	20000	

Bridge

Bridge Ports Port Extensions VLANs MSTIs Port MST Overrides Filters NAT Hosts MDB

MVRP Attributes

Bridge	VLAN IDs	Current Tagged	Current Untagged
;;; added by pvid			
bridge1	1		bridge1, ether2
bridge1	111	bridge1, ether2	
;;; added by vlan on bridge			
bridge1	112	bridge1, ether2	

```
/interface bridge
add name=bridge1 vlan-filtering=yes
/interface bridge port
add bridge=bridge1 interface=ether1
add bridge=bridge1 interface=wifi1 pvid=111
add bridge=bridge1 interface=wifi2 pvid=111
add bridge=bridge1 horizon=10 interface=wifi3 pvid=112
add bridge=bridge1 horizon=10 interface=wifi4 pvid=112
/interface bridge vlan
add bridge=bridge1 tagged=bridge1,ether1 vlan-ids=111
add bridge=bridge1 tagged=bridge1,ether1 vlan-ids=112
```

► WifiWave2 wifi-qcom

- Устройства с wifi-qcom поддерживают передачу VLAN от контроллера
- `/interface wifi cap set discovery-interfaces=bridge1 enabled=yes slaves-datapath=datapath2-guest`
- Для физических интерфейсов необходимо назначать datapath в настройках интерфейса
- Необходим bridge

CAP

☒ Enabled

Discovery Interfaces: bridge1

Certificate:

CAPsMAN Addresses:

CAPsMAN Names:

CAPsMAN Certificate Common Names:

Lock To CAPsMAN:

Slaves Static:

Slaves Datapath: datapath2-guest

Requested Certificate:

Locked CAPsMAN Common Name:

Current CAPsMAN address:

Current CAPsMAN Identity: CAPsMAN

OK

Cancel

Apply

► WifiWave2 wifi-qcom

```
/interface bridge
add name=bridge1 port-cost-mode=short protocol-mode=none
/interface wifi datapath
add bridge=bridge1 disabled=no name=datapath1
add bridge=bridge1 bridge-horizon=10 disabled=no name=datapath2-guest
/interface wifi
set [ find default-name=wifi1 ] configuration.manager=capsman-or-local .mode=ap datapath=datapath1 disabled=no
set [ find default-name=wifi2 ] configuration.manager=capsman-or-local .mode=ap datapath=datapath1 disabled=no
/interface bridge port
add bridge=bridge1 interface=ether1 internal-path-cost=10 path-cost=10
add bridge=bridge1 interface=ether2 internal-path-cost=10 path-cost=10
/interface wifi cap
set discovery-interfaces=bridge1 enabled=yes slaves-datapath=datapath2-guest
/ip dhcp-client
add interface=bridge1
```

Выводы

► WifiWave2 CAPsMAN

- Идет активная разработка и скорее всего будут изменения в настройках
- Уже сейчас возможно получить преимущества использования новых технологий, которые улучшают пользовательский опыт
- Возможно использовать устройства, которые изначально не поддерживали данный пакет
- Если выбирать между новым и более старым CAPsMAN – однозначно новый
- Нет CAPsMAN forwarding
- Приходится поддерживать два варианта конфигураций
- Сложности с мощностью и региональными настройками
- На одном оборудовании не возможно использовать старый и новый CAPsMAN
- Локальные интерфейсы не работают с CAPsMAN

► Полезные ссылки

- <https://help.mikrotik.com/docs/pages/viewpage.action?pageId=46759946>
- <https://www.youtube.com/watch?v=15pCATqqJww>
- <https://www.youtube.com/watch?v=AkBIQxi-VKs>
- <https://www.youtube.com/watch?v=r2OxOYM0IlQ&t>

Выражаем благодарность за возможность встречаться с вами очно



Точке Кипения "Техноград ВДНХ", а именно:

- Алексею Дерябкину
- Денису Устинову





Презентация

<http://mkrtk.ru/wb0724capm>

Спасибо за внимание!

Пишите свои вопросы в чат Telegram:
@MikTrain

Мои контакты:

Роман Козлов

trainer@mikrotik-training.ru

+7 495 256-9-256

Telegram: **@soriel**