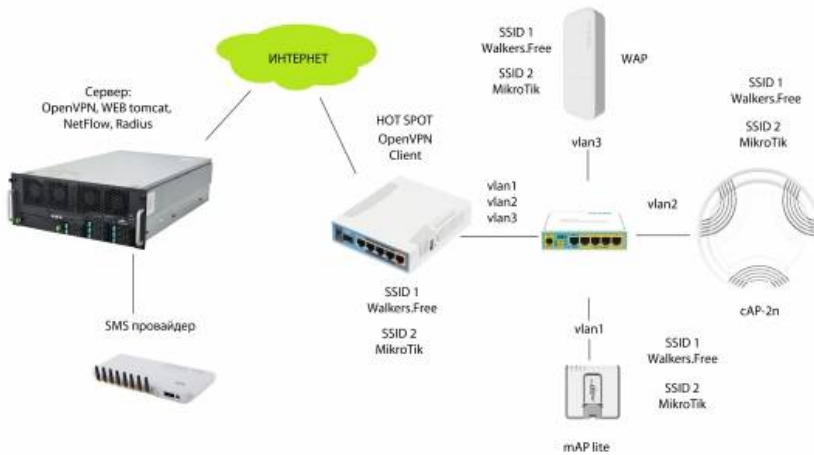
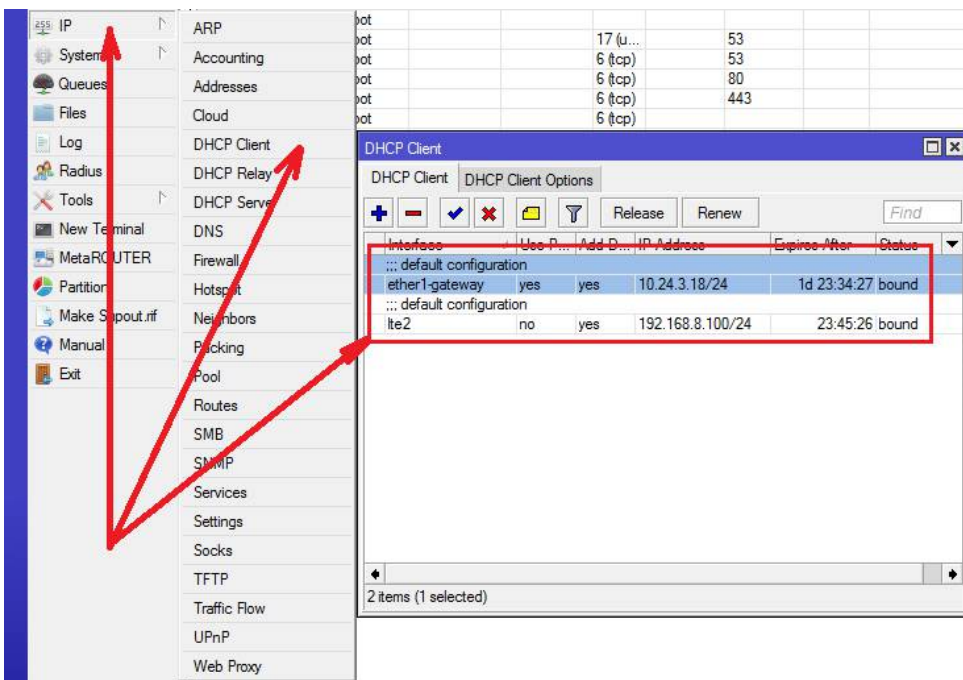


Настройка системы SMS авторизации iGoFree на MikroTik

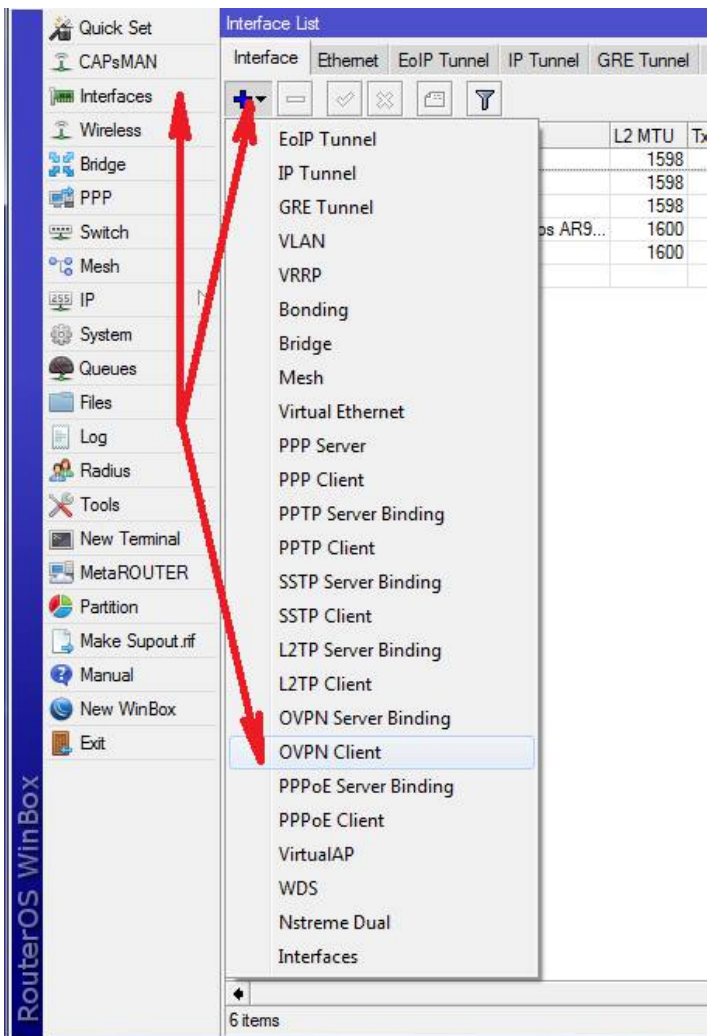


Данная статья содержит материалы со встречи пользователей MikroTik в Минске 3 июня 2016 года. Это выступление Кардаша Александра Владимировича на MUM Belarus 2016 о настройке системы SMS авторизации через сервис iGoFree на оборудовании MikroTik. Содержит типовую схему внедрения сервиса компании ООО "Уолкерс Системс" в сетевую инфраструктуру мест, где необходимо организовать публичный доступ к интернету через Wi-Fi сеть. Слайды с презентации Евгения Осипова можно скачать по [этой ссылке](#).

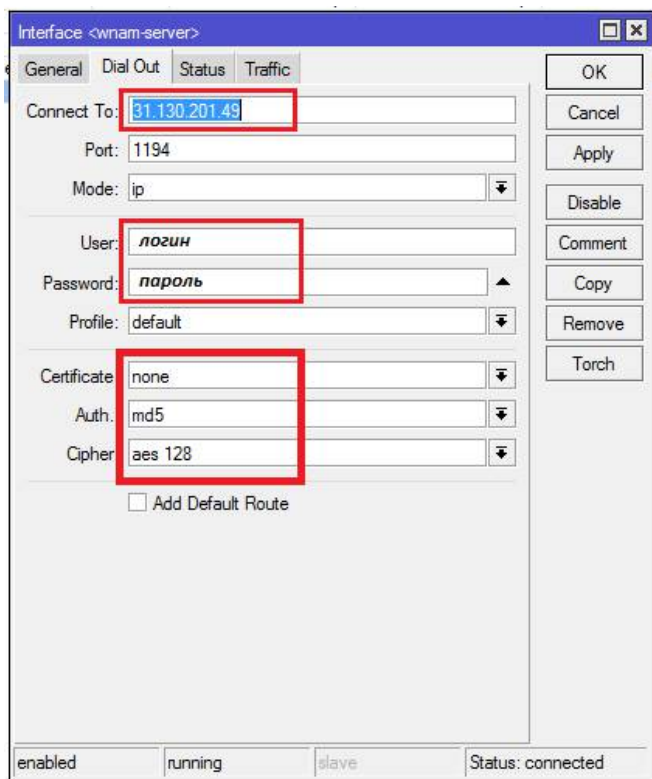
Настройка начинается с подключения маршрутизатора к интернету. В самом простом случае следует вставить Ethernet кабель от провайдера в первый порт MikroTik и роутер получает IP через **DHCP client**. Кроме того по умолчанию на первом порту сделан **scr-nat masquerade**. Если необходима постоянная доступность интернета, можно настроить резервирование через 3G модем. С модемами Huawei поддерживающими Hi-Link нужно создать **DHCP client** на интерфейсе **lte2** указав в поле **Default Route Distance** (метрика или цена маршрута) значение большее чем на основном канале. Далее следует сделать IP/Firewall/NAT правило **scr-nat** action **Masquerade** на интерфейс **lte2** созданный 3G модемом.



Настроим OpenVPN client на MikroTik. Для этого откроем окно с интерфейсами и плюсиком добавим новый интерфейс:

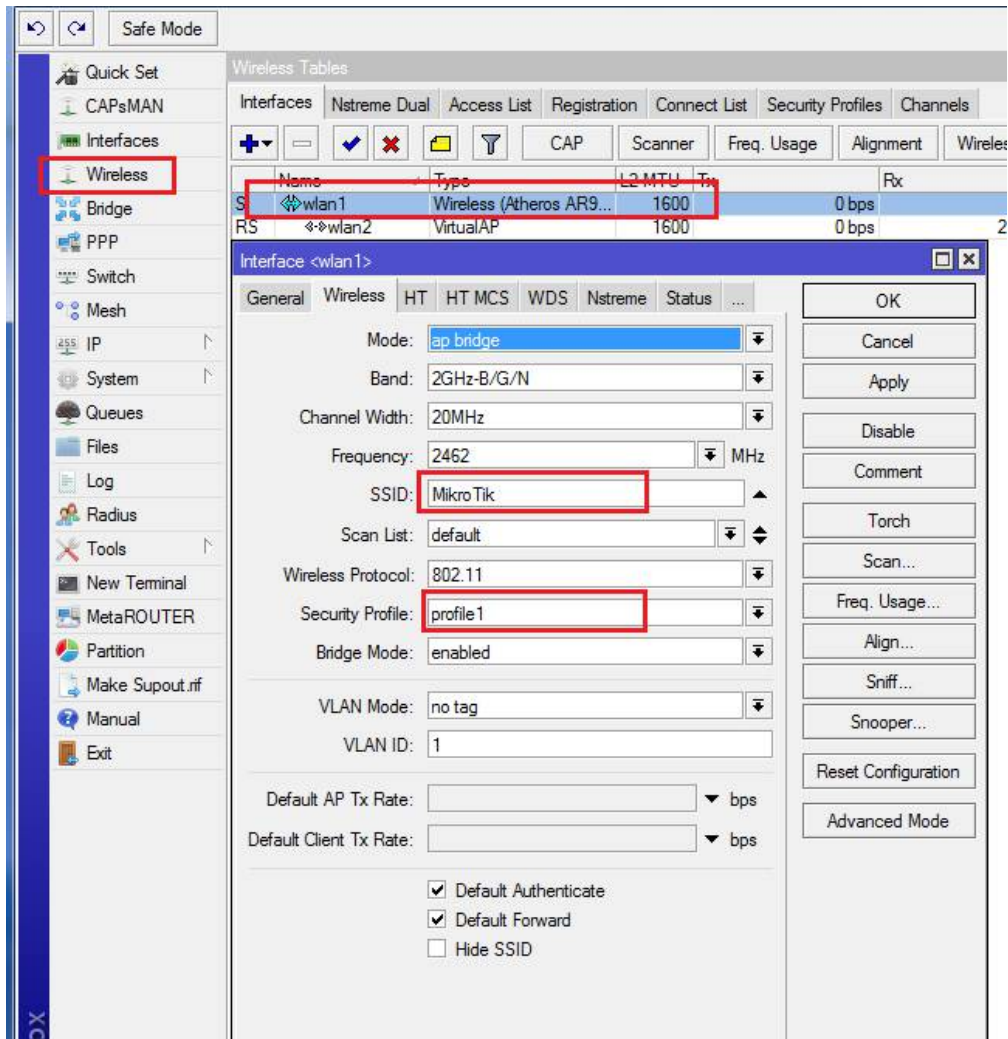


Введём IP адрес сервера OpenVPN и логин пароль для доступа к нему. Хэшкод MD5 и алгоритм шифрования AES с ключём 128 бит:

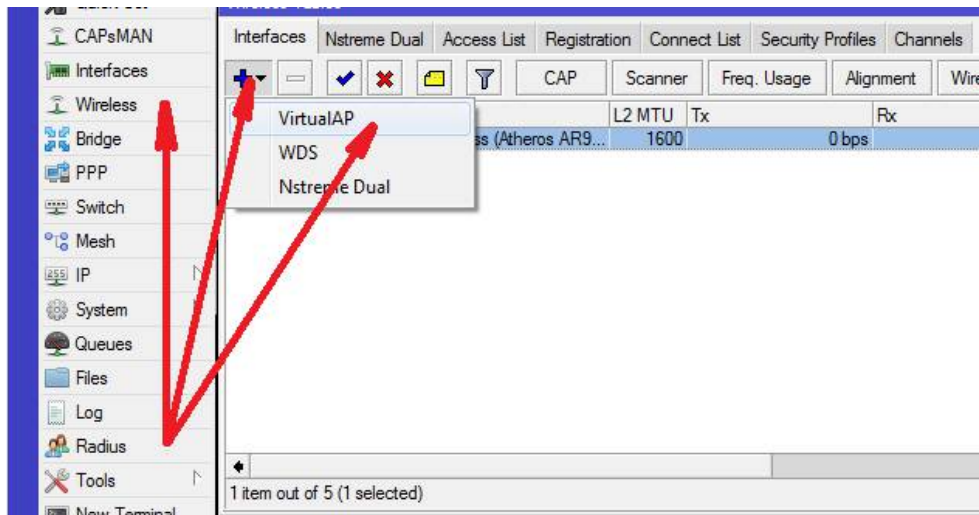


Настроим точку доступа wlan1 вещающую Wi-Fi сеть персонала заведения в котором устанавливается система авторизации. Выбираем узкие каналы в 20 mHz которые позволяют достиг максимальной дальности Wi-Fi сигнала. Связано это с тем, что энергия точки доступа распределяется на более узкую полосу, позволяя иметь в два раза большую силу сигнала на удалённых участках сети. Иначе сказать полезный сигнал Wi-Fi будет сильнее выделяться на уровне шумов. Кроме того на узких каналах можно разместить больше точек доступа разнеся их даже на 1, 5, 9, 13 канал максимально заполнив радиочастотный спектр полезным сигналом. Выбрав **Wireless Protocol 802.11** можно обеспечить максимальную совместимость с Wi-Fi устройствами клиентов заведения, ведь обычные

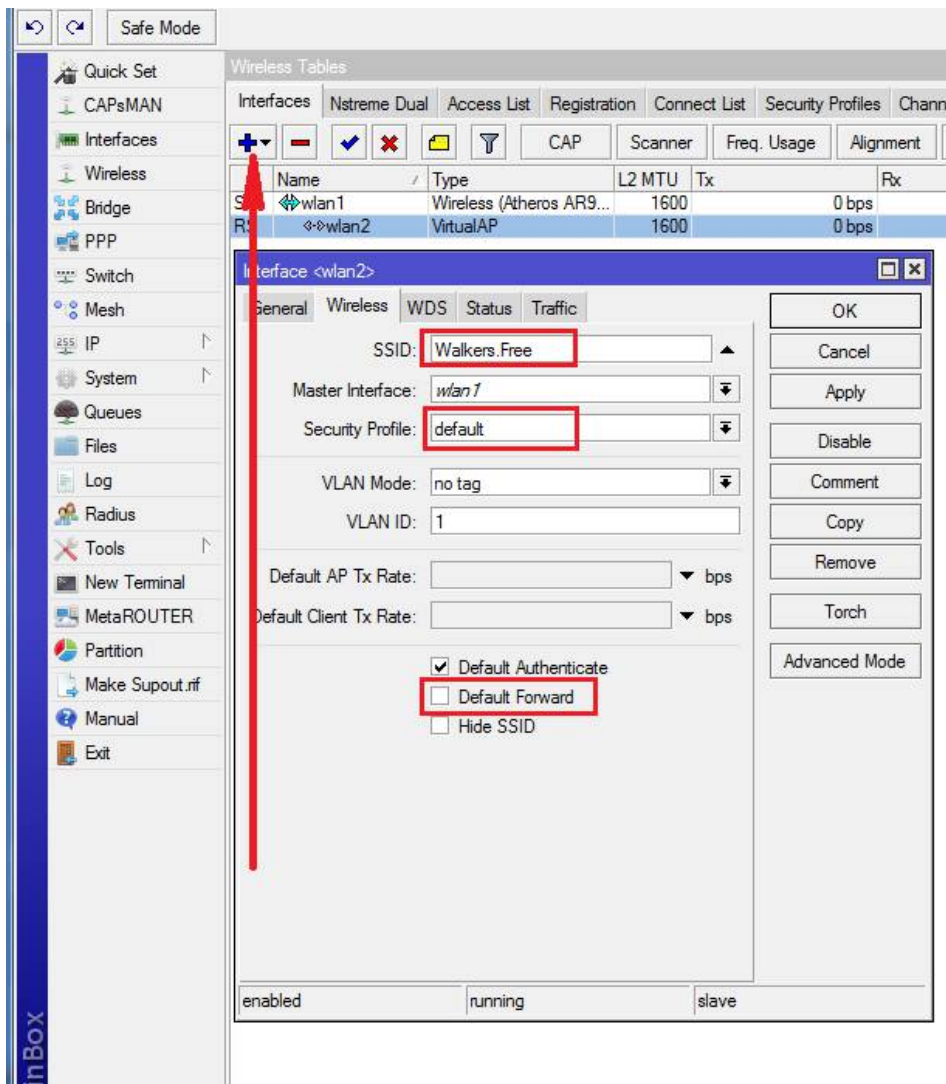
устройства не поддерживают проприетарных полинговых проколов MikroTik.



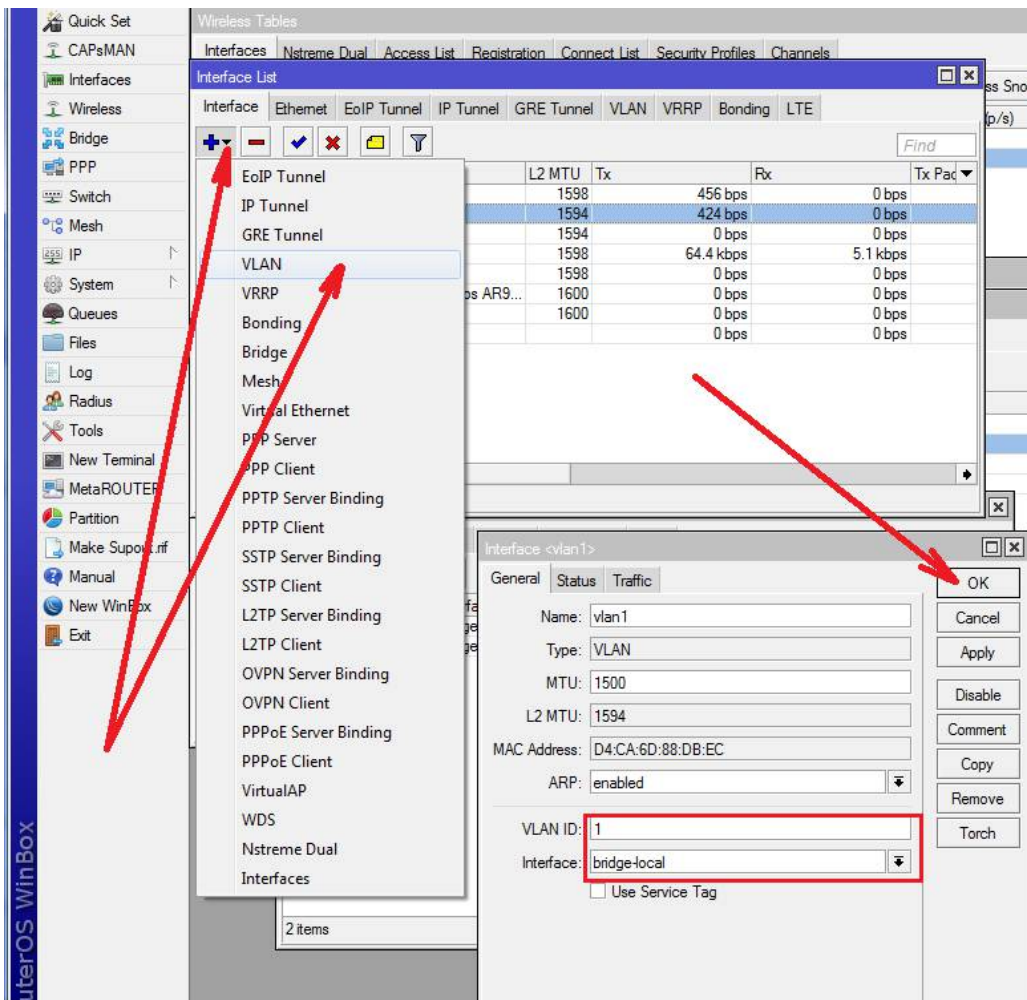
Создадим виртуальную точку доступа Wi-Fi в которой будет использоваться SMS авторизация:



Индикатор сети **SSID Walkers.Free** профиль сети **default**, который не содержит пароля. Чтобы предотвратить ARP спуфинг клиентов друг другом (атака человек по середине позволяющая перехватывать трафик пользователя не использующего шифрования) снимаем галочку **Default Forward** и тем самым запрещаем передавать данные между клиентами подключенными к свободной Wi-Fi сети.



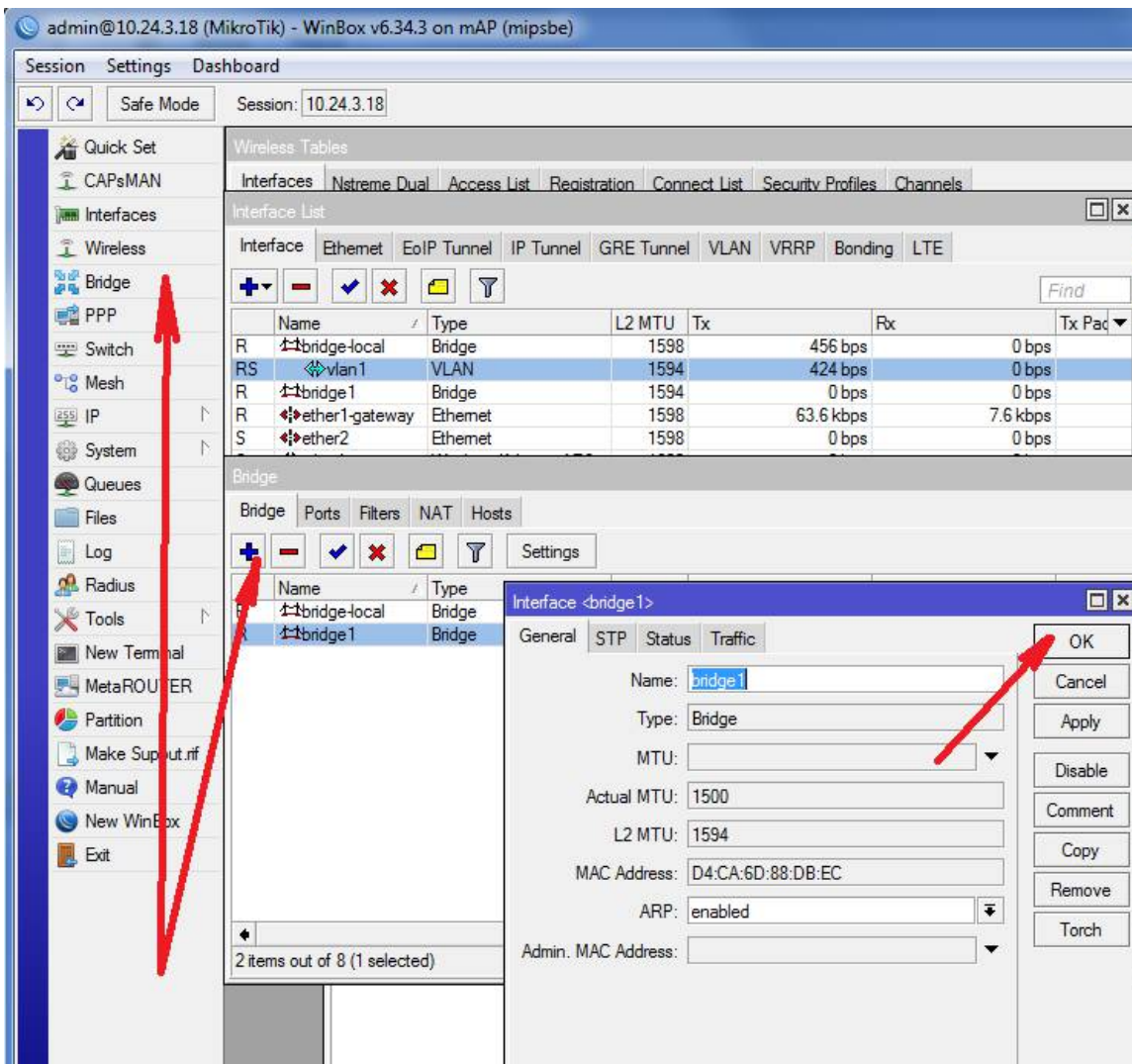
Мы хотим сделать одну сеть с индикатором Walkers.Free на четырёх точках доступа Wi-Fi позволяющую использовать SMS авторизацию. Проще всего это сделать с помощью технологии VLAN на основе меток. Кадры основной сети не будут иметь меток, а кадры дополнительной будут помечаться id 1, 2, 3. Создаём wlan1 с id 1 на интерфейсе **bridge-local**:



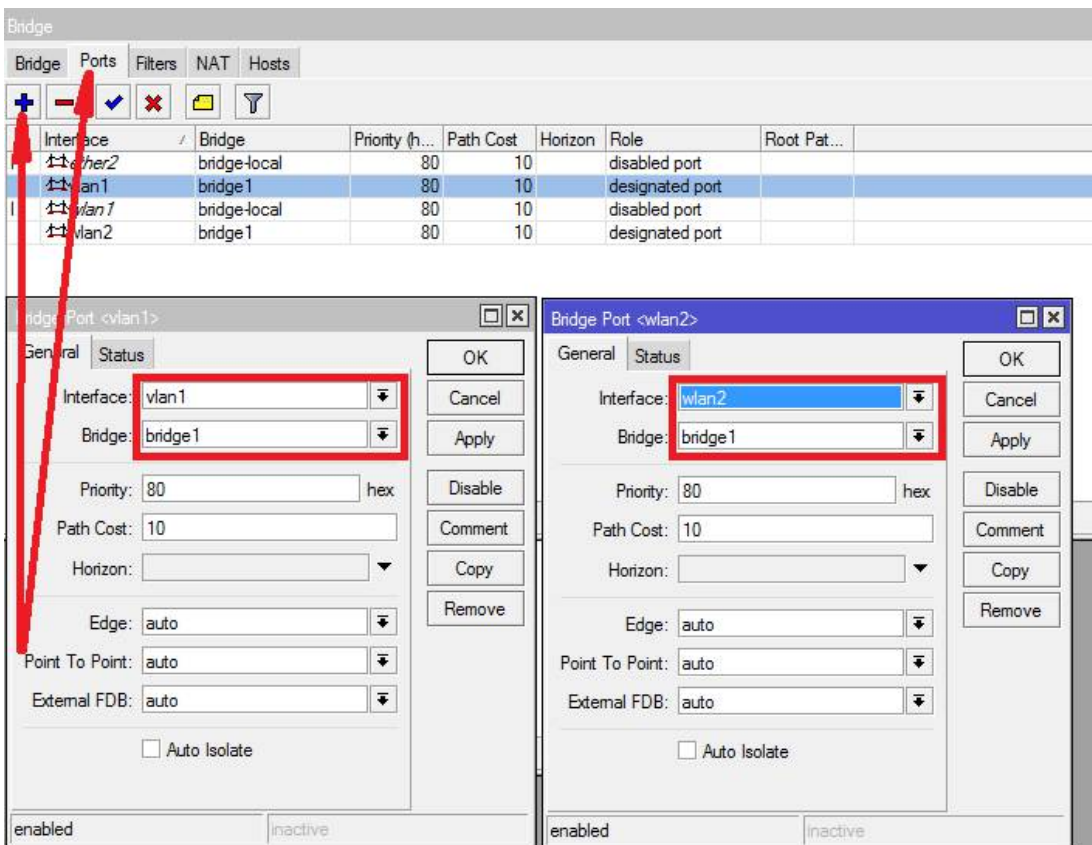
По аналогии создаём **vlan2** с id 2 и **vlan3** с id 3:

Interface	Name	Type	L2 MTU	Tx	Rx	Tx Pac
R	bridge-local	Bridge	1598	80.0 kbps	4.6 kbps	
RS	vlan1	VLAN	1594	424 bps	0 bps	
RS	vlan2	VLAN	1594	424 bps	0 bps	
RS	vlan3	VLAN	1594	424 bps	0 bps	
R	bridge1	Bridge	1594	0 bps	0 bps	
R	ether1-gateway	Ethernet	1598	14.5 kbps	6.5 kbps	
RS	ether2	Ethernet	1598	86.0 kbps	19.1 kbps	
R	lte2	LTE		0 bps	0 bps	
R	to-server	OVPN Client		128 bps	0 bps	
R	to-traffic-flow	PPTP Client		0 bps	0 bps	
S	wlan1	Wireless (Atheros AR9...	1600	0 bps	0 bps	
RS	wlan2	VirtualAP	1600	0 bps	0 bps	

Создадим **bridge1** на котором будет работать хотспот:



Добавим в **bridge1** **vlan1**, **vlan2**, **vlan3** и виртуальную точку доступа Wi-Fi **wlan2**:



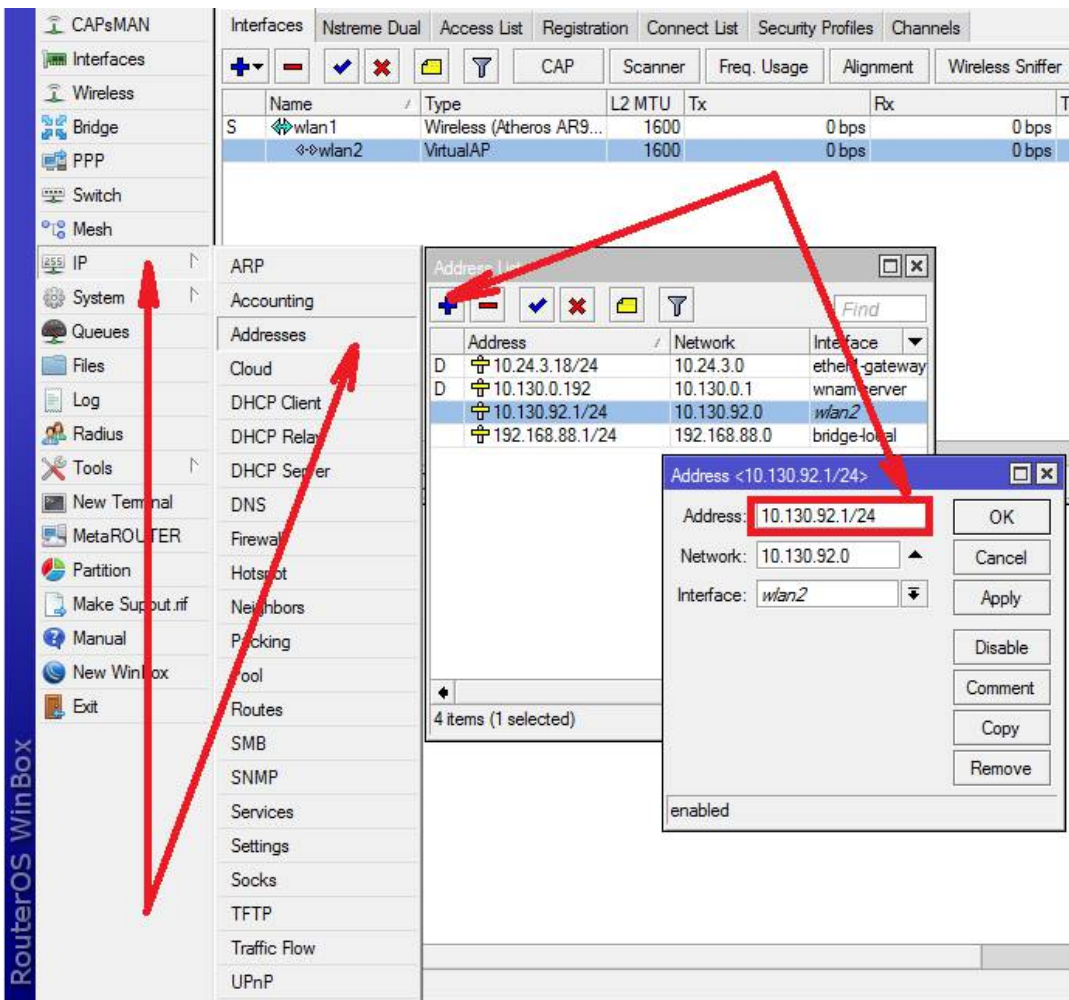
Зафильтруем на вкладке **Filters** трафик между **vlan1**, **vlan2**, **vlan3** и **wlan2**, чтобы клиенты подключённые к разным точкам доступа не могли передавать данные между собой:

The screenshot shows the Mikrotik WinBox interface for configuring a Bridge Filter Rule. The main window displays a table of filter rules:

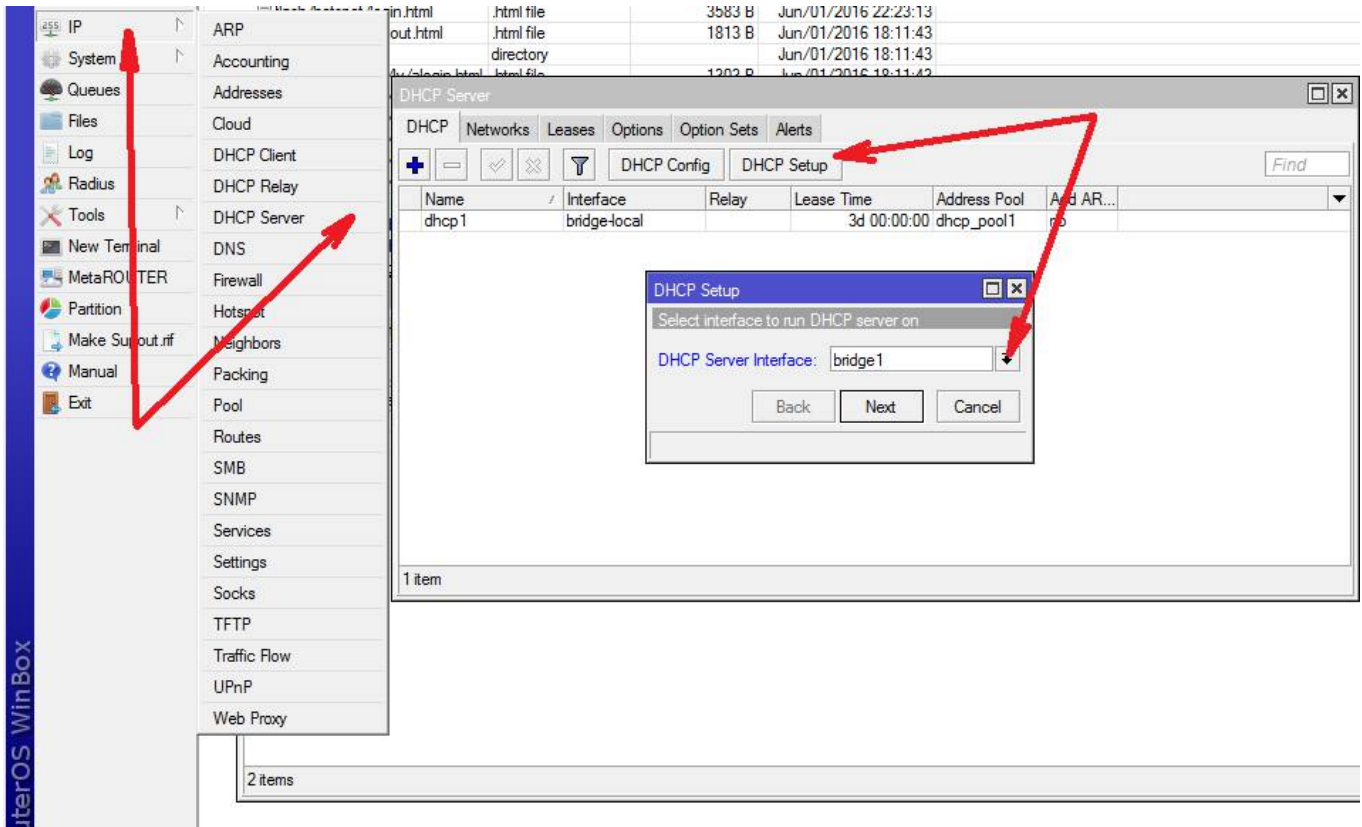
#	Chain	Interface/In-Interface	Interface/Out-Interface	Src. MAC Address...	Dst. MAC Address...	MAC Prot...	Bytes	Packets
0	forward	vlan1	vlan1				0	0
1	forward	vlan2	vlan2				0	0
2	forward	wlan2	wlan2				0	0
3	forward	vlan3	vlan3				0	0

The 'Bridge Filter Rule' dialog box is open, showing the 'Action' dropdown menu set to 'drop'. The dialog also includes options for 'Log', 'Log Prefix', and buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters'. The status at the bottom of the dialog is 'enabled'.

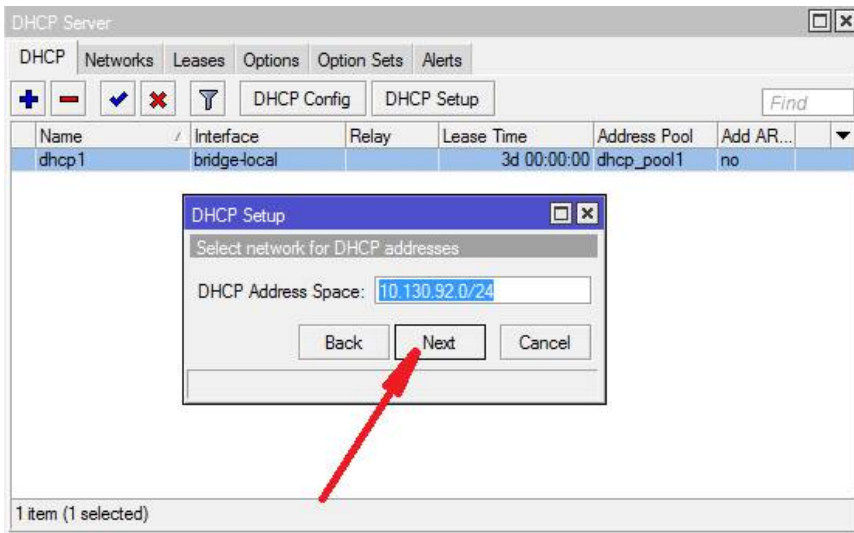
Пропишем IP адрес на интерфейсе на котором мы будем делать HotSpot. В нашем случае это bridge1 хотя можно прописать и на wlan2:



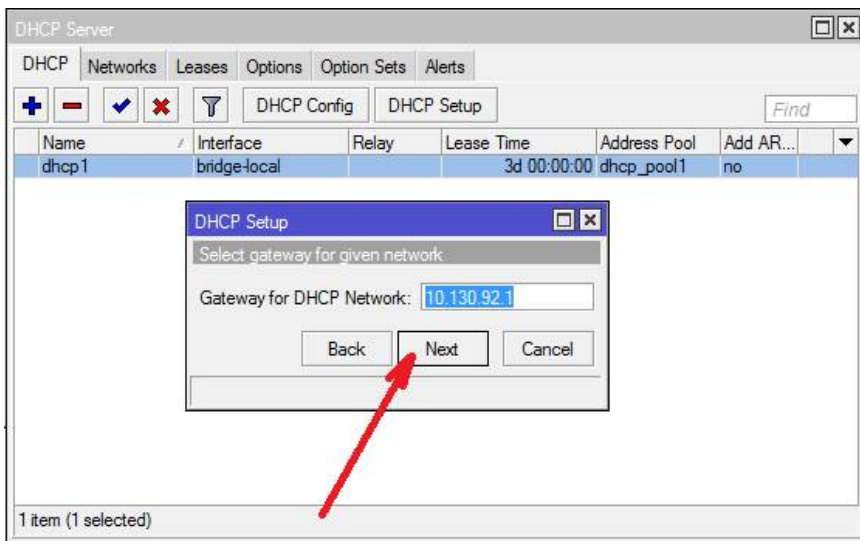
Настроим с помощью мастера DHCP сервер:



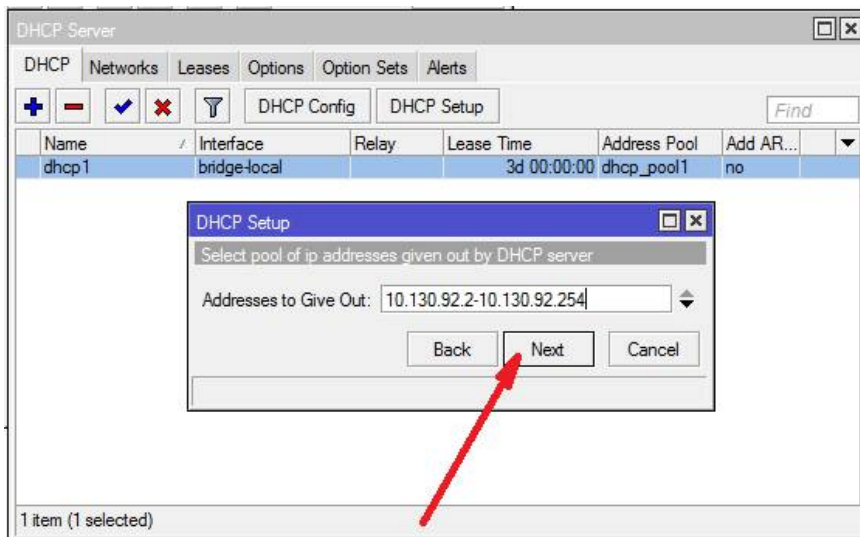
Согласимся с предложенной сетью 10.130.92.0/24:



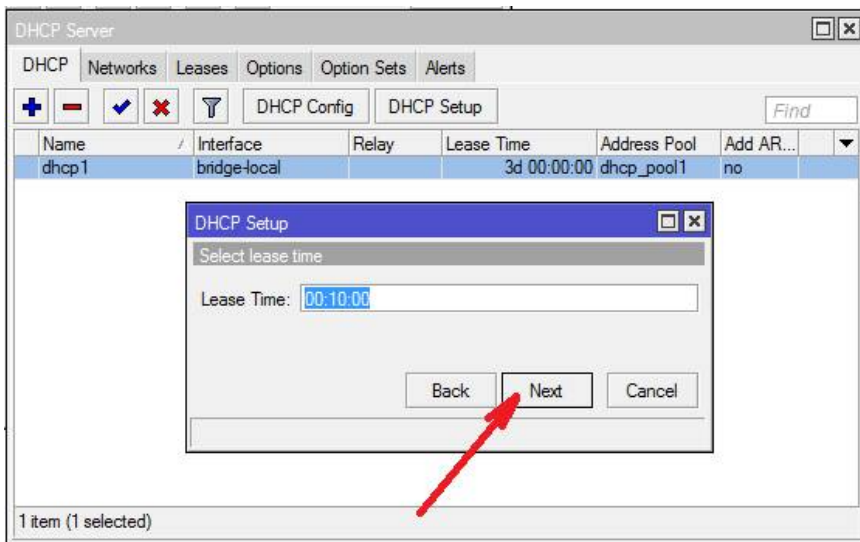
Согласимся с предложенным мастером шлюзом:



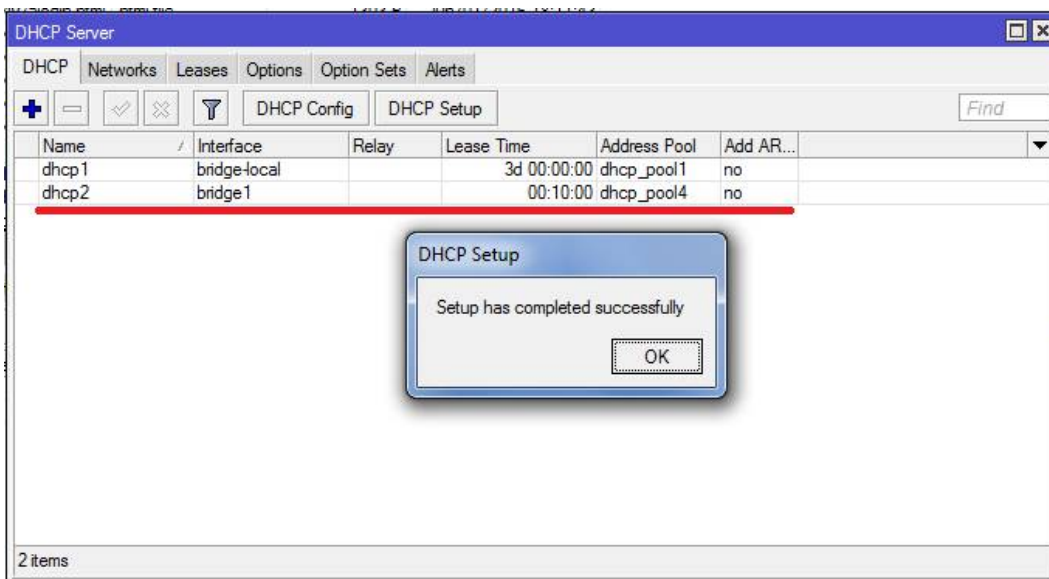
Ввиду того, что в свободной сети Walkers.Free не будет размещаться сетевое оборудование можно использовать весь пул свободных IP адресов кроме 10.130.92.1:



Время аренды IP адреса по умолчанию 10 минут, нажмём Next ничего не меняя:



Если всё правильно сделано мы увидим сообщение, что DHCP успешно настроен:



В сети персонала рекомендую выставить DHCP "authoritative" в Yes (DHCP авторитетный - Да), что заставит DHCP отвечать на запросы клиентов максимально быстро и отключить неавторитетные DHCP сервера в сети. Также выставить галочку "Add ARP for leases" для того чтобы в ARP таблицу автоматически добавлялись сопоставления IP с MAC.

DHCP Server

DHCP Networks Leases Options Option Sets Alerts

DHCP Config DHCP Setup Find

Name	Interface	Relay	Lease Time	Address Pool	Add AR...
dhcp1	bridge-local		3d 00:00:00	dhcp_pool1	no
dhcp2	bridge1		00:10:00	dhcp_pool4	yes

2 items (1 selected)

DHCP Server <dhcp2>

Name: dhcp2 OK

Interface: bridge1 Cancel

Relay: Apply

Lease Time: 00:10:00 Disable

Bootp Lease Time: forever Copy

Address Pool: dhcp_pool4 Remove

Src. Address: Delay Threshold: Authoritative: yes

Bootp Support: after 2s delay

Lease Script: after 10s delay

no

yes

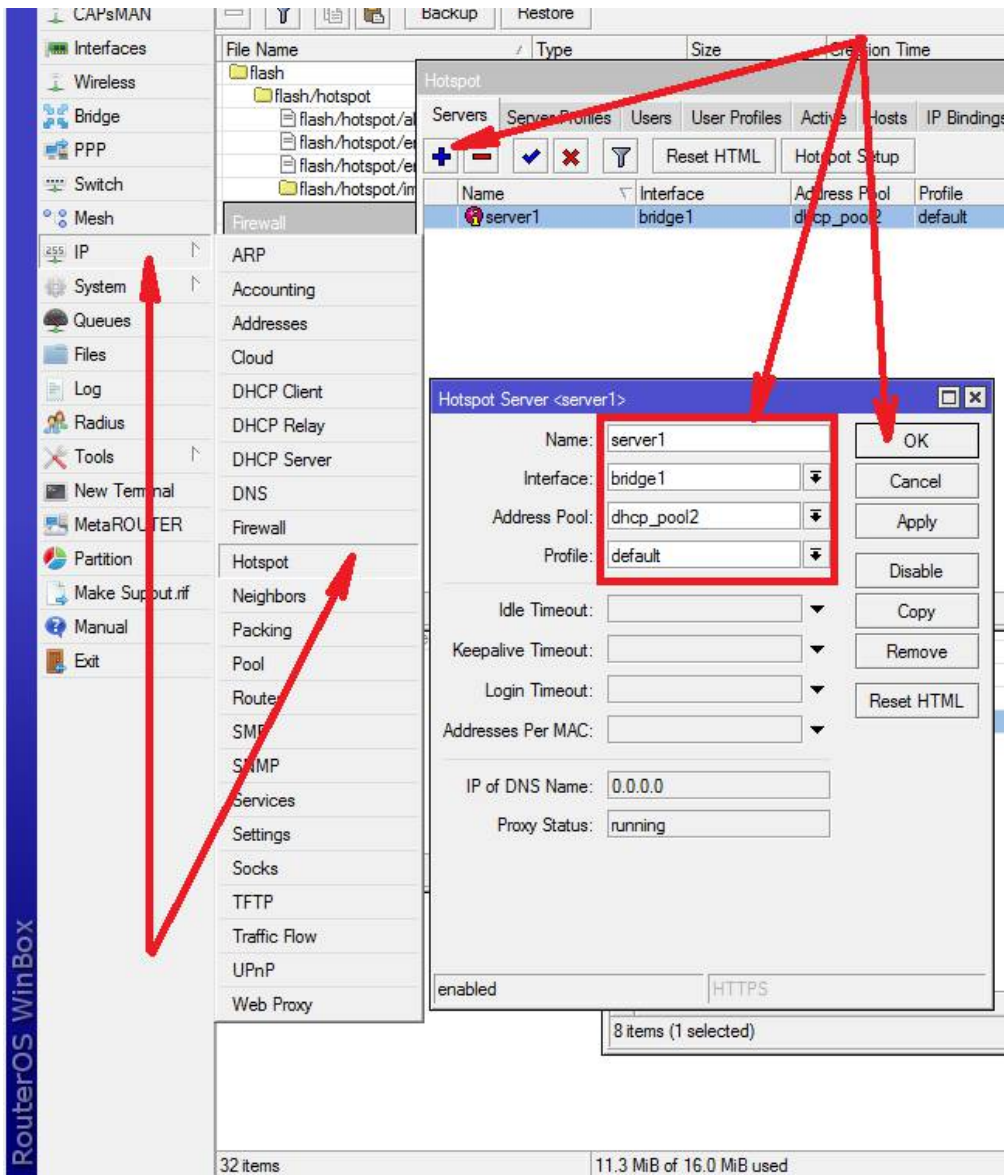
Add ARP For Leases

Always Broadcast

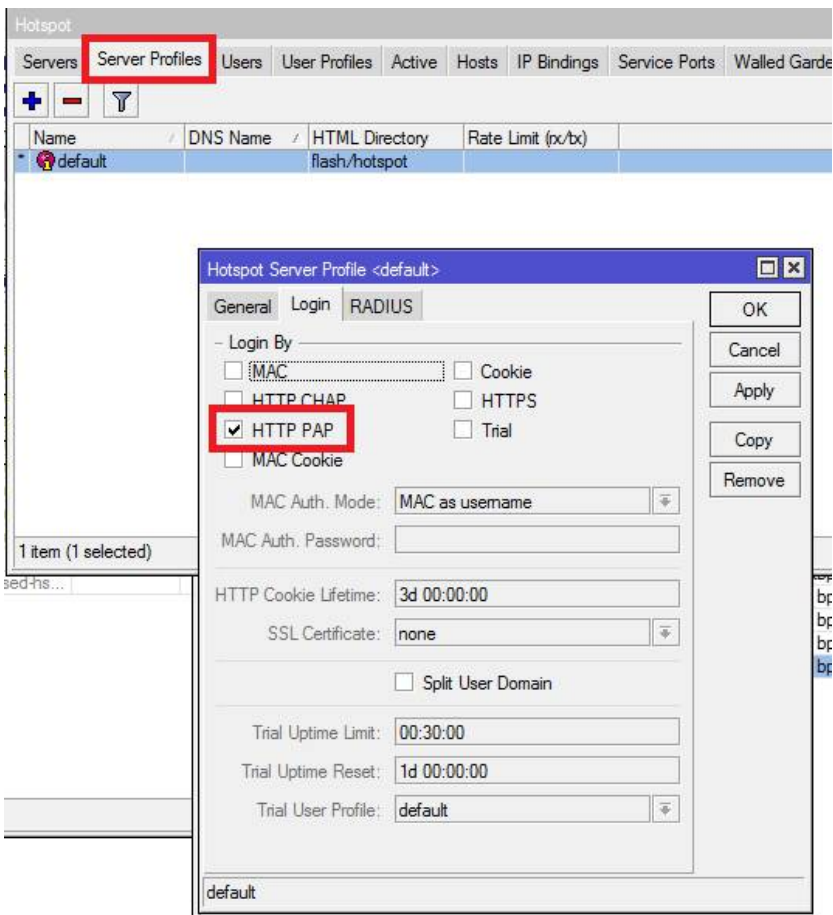
Use RADIUS

enabled

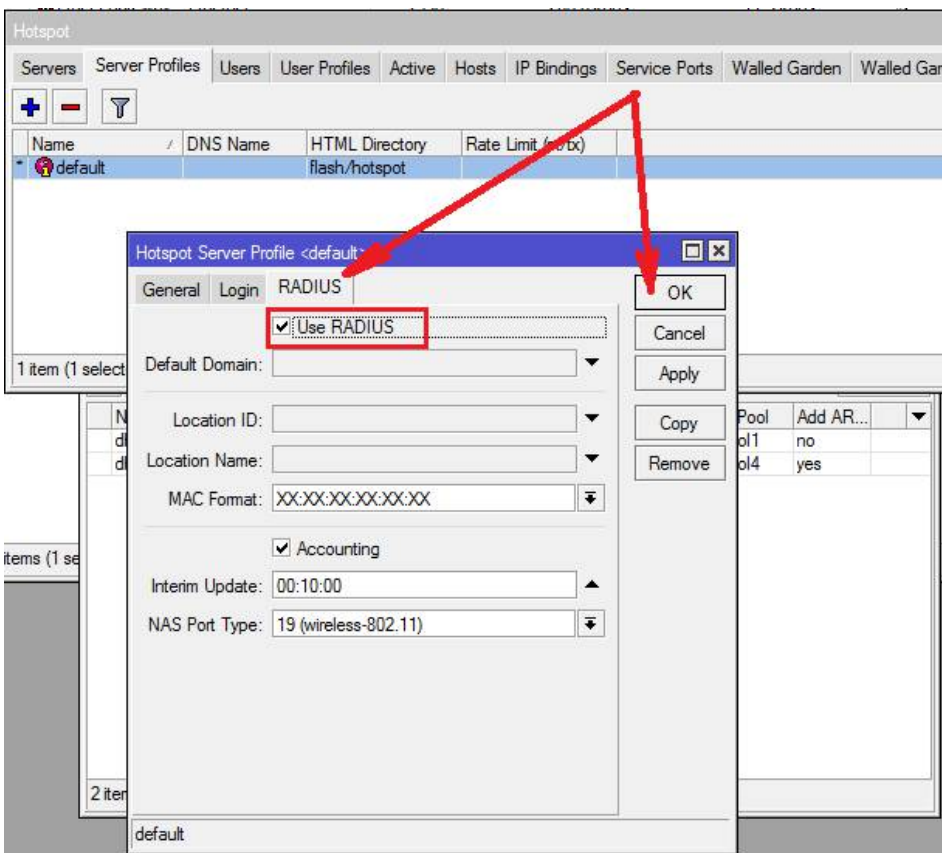
Настроим HotSpot. Если его нет в меню IP, значит необходимо зайти в System/Packages, включить его и программно перезагрузить маршрутизатор. Если он уже включён, открываем окно создания HotSpot и плюсиком создаём новый сервер: Выбираем интерфейс на котором будет работать HotSpot - **bridge1**; пул раздачи IP адресов ранее созданный с помощью мастера настройки DHCP и профиль **default**, который сейчас будем править:



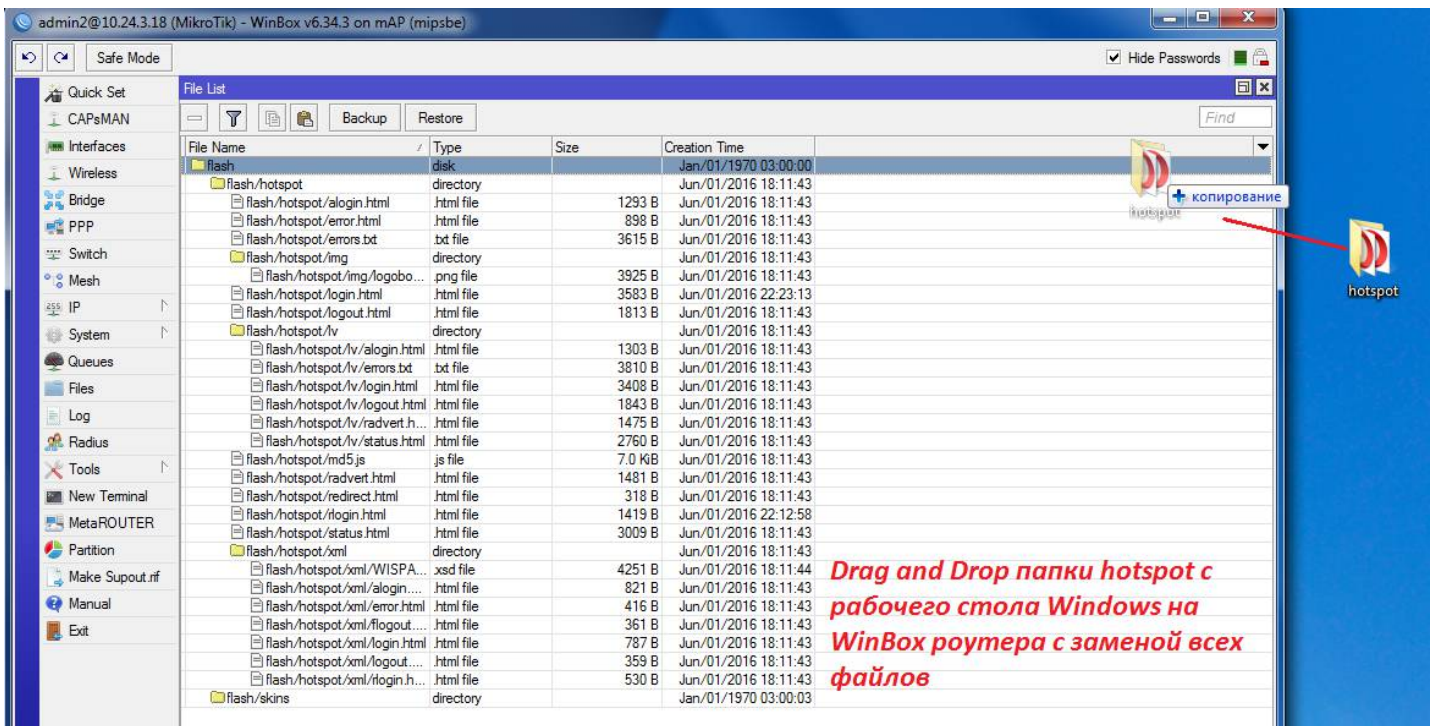
Поправим Server Profile **default**: Ставим галочку Login HTTP PAP. Данные для авторизации пользователя можно передавать открытым текстом по сети ввиду того, что ARP спуфинг не возможен.



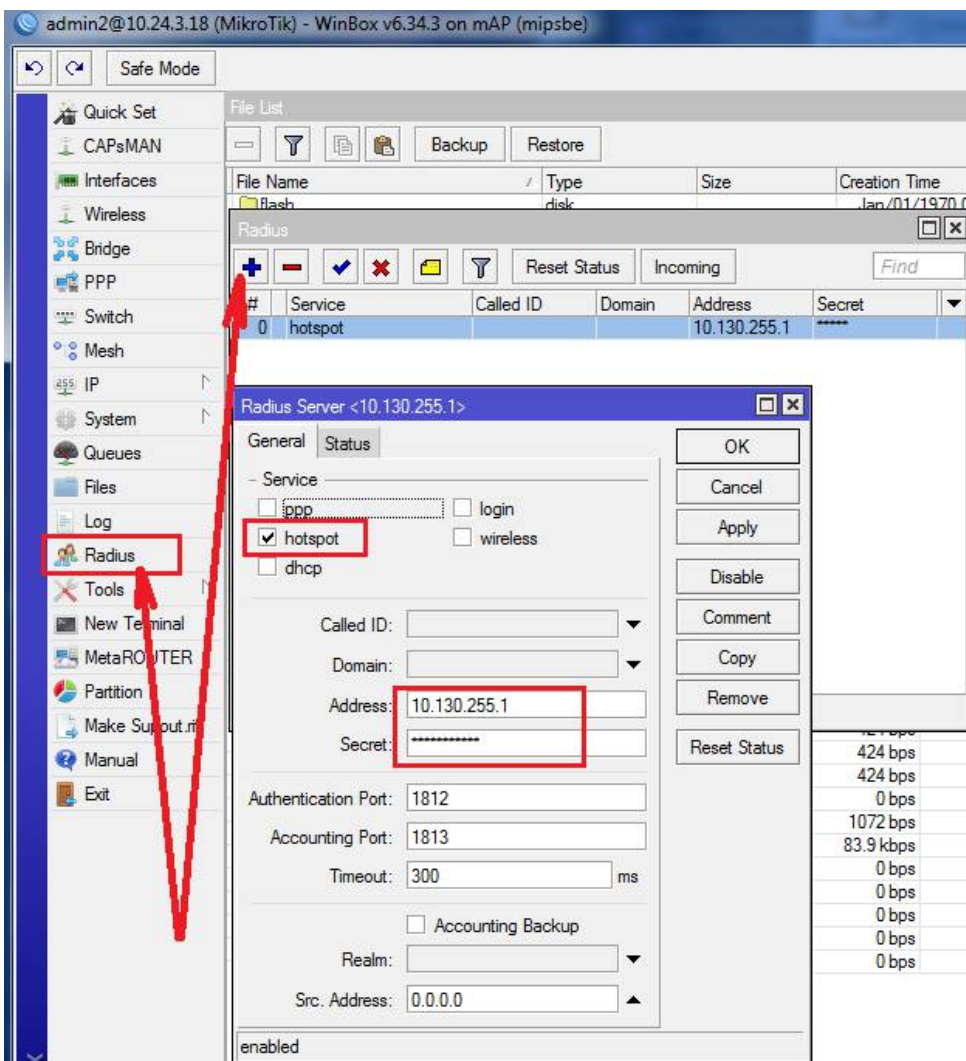
На вкладке **RADIUS** поставим галочку **Use RADIUS**, что означает что список пользователей (MAC адресов) будет храниться на радиус сервере ООО "Уолкерс Системс":



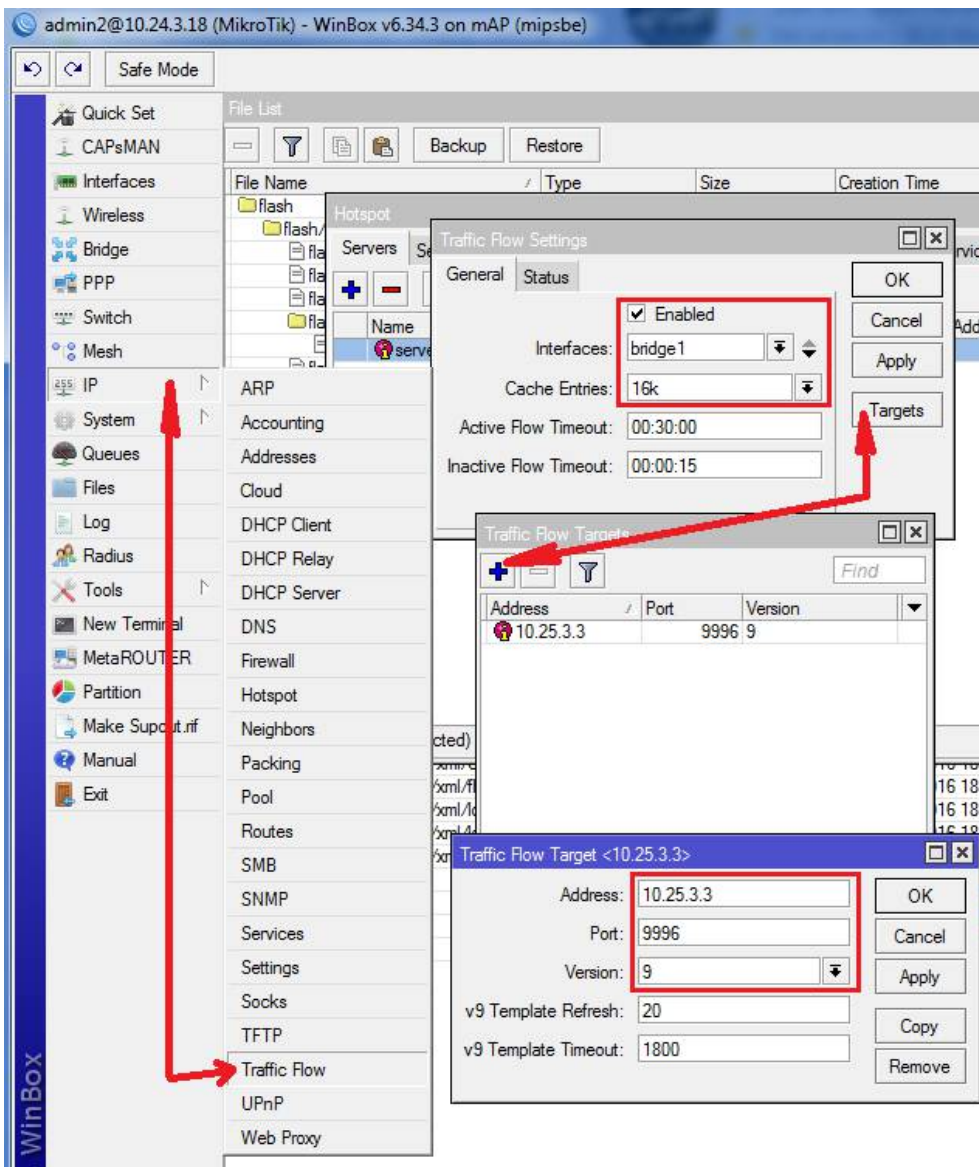
Добавим список хостов и IP адресов к которым разрешён доступ без авторизации на HotSpot, чтобы пользователи могли увидеть страничку авторизации:



Номера телефонов и MAC адреса пользователей хранятся на FreeRadius сервере. Настроим подключение роутера к серверу. Укажем IP адрес его, сервис для которого он используется и пароль:



Сведения о трафике пользователей собираются на внешнем сервере (коллекторе) работающим с протоколом **netflow**. В данном примере показана работа по протоколу 9-ой версии. Включим сенсор netflow на роутере поставив галочку в поле **Enable**. Выберем интерфейс с которого нужно собирать статистику, для того чтобы в анализаторе не было дублированных данных выбираем только интерфейс на котором есть наши пользователи. Нажав кнопку Target добавляем IP адреса серверов (коллекторы **netflow**). Собирать данные можно на нескольких серверах. Данные которые можно увидеть в анализаторе будут содержать IP адрес, протокол и порт по которому происходит передача данных от пользователя и к нему. Также собираются сведения о количестве трафика и времени использования интернета.



Следует сделать также **scr-nat** с Action **masquerade** на интерфейс ведущий к серверам: FreeRADIUS, NetFlow коллектору:

The screenshot shows the Mikrotik WinBox Firewall configuration interface. The left sidebar contains a menu with 'Firewall' selected. The main window displays a table of Firewall Filter Rules. Rule 17 is highlighted in blue. Below the table, the 'NAT Rule' configuration window is open, showing the 'Chain' set to 'srcnat' and the 'Out. Interface' set to 'to-server'. Red arrows point from the 'Chain' and 'Out. Interface' fields in the NAT Rule window to the corresponding columns in the Firewall Filter Rules table.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Interface
0	D	jump		dstnat					
1	D	jump		hotspot					
2	D	jump		hotspot					
3	D	jump		hotspot	17 (u...		53		
4	D	jump		hotspot	6 (tcp)		53		
5	D	jump		hotspot	6 (tcp)		80		
6	D	jump		hotspot	6 (tcp)		443		
7	D	jump		hotspot	6 (tcp)				
8	D	jump		hs-unauth	6 (tcp)		80		
9	D	jump		hs-unauth	6 (tcp)		3128		
10	D	jump		hs-unauth	6 (tcp)		8080		
11	D	jump		hs-unauth	6 (tcp)		443		
12	D	jump		hs-unauth	6 (tcp)		25		
13	D	jump		hs-auth	6 (tcp)				
14	D	jump		hs-auth	6 (tcp)		25		
... place hotspot rules here									
15	X	pas...		unused-hs...					
16		mas...		srcnat					ether1-gateway
17		mas...		srcnat					to-server
18		mas...		srcnat					to-traffic-flow

The NAT Rule configuration window shows the following fields:

- Chain: srcnat
- Src. Address: [empty]
- Dst. Address: [empty]
- Protocol: [empty]
- Src. Port: [empty]
- Dst. Port: [empty]
- Any. Port: [empty]
- In. Interface: [empty]
- Out. Interface: to-server
- Packet Mark: [empty]
- Connection Mark: [empty]
- Routing Mark: [empty]

Можно также обратить внимание на правила с буквой D (от dynamic), автоматически добавленные HotSpot:

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Interface
0	D	jump	dstnat						
1	D	jump	hotspot						
2	D	redir...	hotspot			17 (u...	53		
3	D	redir...	hotspot			6 (tcp)	53		
4	D	redir...	hotspot			6 (tcp)	80		
5	D	redir...	hotspot			6 (tcp)	443		
6	D	jump	hotspot			6 (tcp)			
7	D	jump	hotspot			6 (tcp)			
8	D	redir...	hs-unauth			6 (tcp)	80		
9	D	redir...	hs-unauth			6 (tcp)	3128		
10	D	redir...	hs-unauth			6 (tcp)	8080		
11	D	redir...	hs-unauth			6 (tcp)	443		
12	D	jump	hs-unauth			6 (tcp)	25		
13	D	redir...	hs-auth			6 (tcp)			
14	D	jump	hs-auth			6 (tcp)	25		
... place hotspot rules here									
15	X	pas...	unused-hs...						
16		mas...	srcnat						ether1-gateway
17		mas...	srcnat						to-server
18		mas...	srcnat						to-traffic-flow

NAT Rule

General Advanced Extra Action Statistics

Action: **masquerade**

Log

Log Prefix: _____

Настроим правила фильтрации трафика. Если на маршрутизаторе реальный (статический) IP адрес в интернете рекомендуем проверить наличие в цепочке input на внешнем интерфейсе разрешающих правил **connection state: established** и **related**. Если необходимо, можно разрешить ICMP, WEBBOX, WINBOX, SSH, Telnet. Остальной трафик к внешнему интерфейсу лучше закрыть действием **drop**, что позволит уменьшить атаки на такие сервисы роутера как DNS и др..

Также следует в цепочке **forward** запретить доступ из сети с SMS авторизацией в сеть персонала и сетевого оборудования 10.130.92.0/24 ->> 192.168.0.0/16 действие **Drop**.

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

Find all

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Int...	Bytes	Packets
0	D	jump	forward							701.5 KiB	2 806
1	D	jump	forward							3922 B	26
2	D	jump	input							160.3 KiB	2 193
3	D	drop	input		6 (tcp)		64872-64875			0 B	0
4	D	jump	hs-input							160.3 KiB	2 193
5	D	acc...	hs-input		17 (udp)		64872			24.5 KiB	391
6	D	acc...	hs-input		6 (tcp)		64872-64875			135.5 KiB	1 797
7	D	jump	hs-input							0 B	0
8	D	reject	hs-unauth		6 (tcp)					8.6 KiB	130
9	D	reject	hs-unauth							692.7 KiB	2 673
10	D	reject	hs-unauth-to							3806 B	25
::: place hotspot rules here											
11	X	pas...	unused-hs...							0 B	0
::: established											
12	D	acc...	input							237.6 KiB	3 895
::: related											
13	D	acc...	input							0 B	0
::: admin											
14	D	acc...	input		6 (tcp)		8291,80,23,22			1903 B	22
::: wan block											
15	D	drop	input					ether1-gateway		2544 B	17
::: wan block											
16	D	drop	input					lte2		516 B	4
::: HotSpot to Lan Drop											
17	D	drop	forward	10.130.92.0/24	192.168.0.0/16					0 B	0
::: invalid											
18	D	drop	forward							0 B	0

19 items (1 selected)

Firewall Rule <10.130.92.0/24->192.168.0.0/16>

General Advanced Extra **Action** Statistics

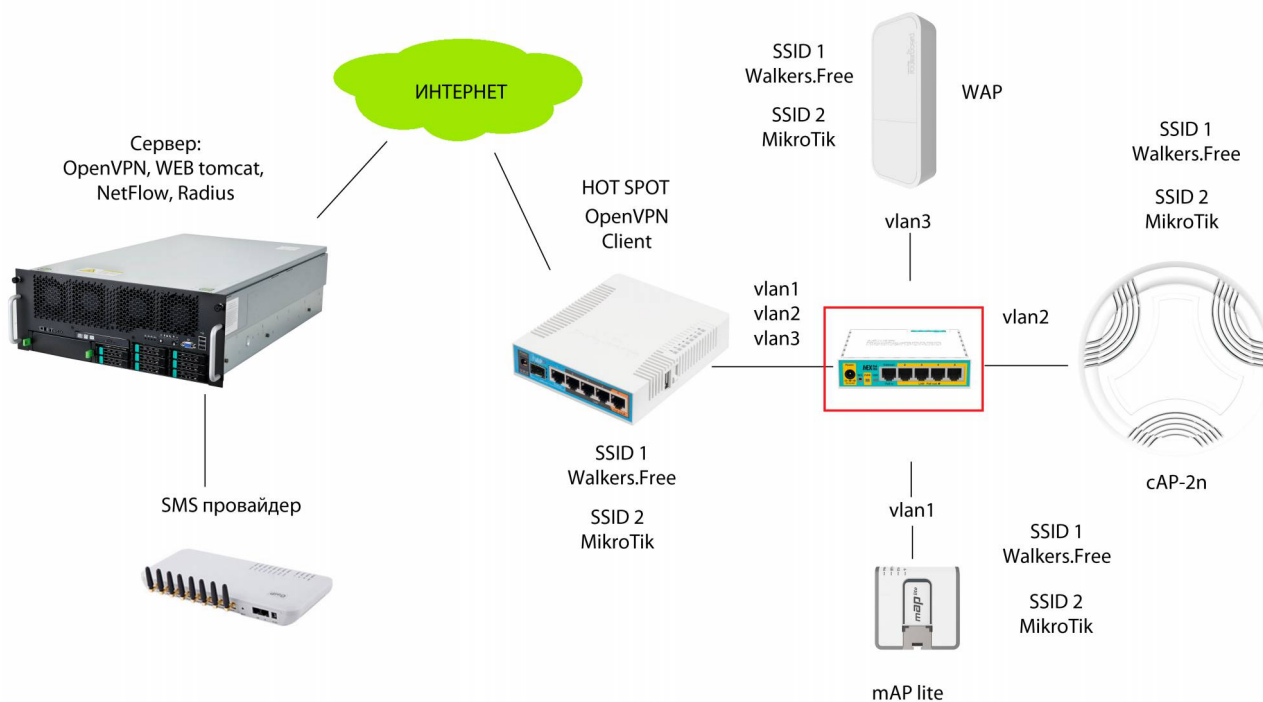
Action: **drop**

Log

Log Prefix: _____

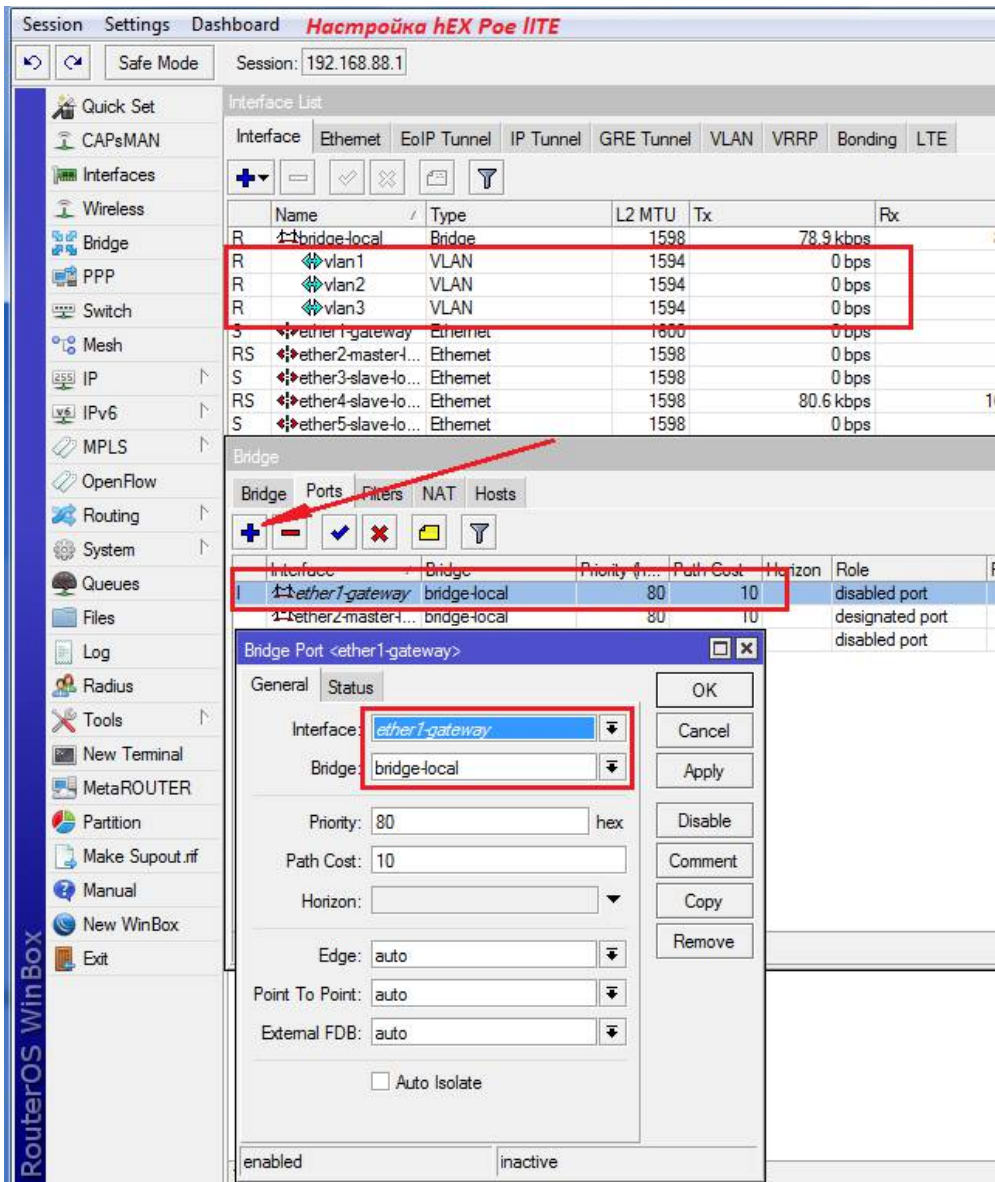
OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

Настроим **hEX PoE lite** поддерживающий пассивный PoE и позволяющий строить недорогие сети в местах где невозможно запитать Wi-Fi точки доступа, кроме как по ethernet кабелю. На схеме он выделен красным:

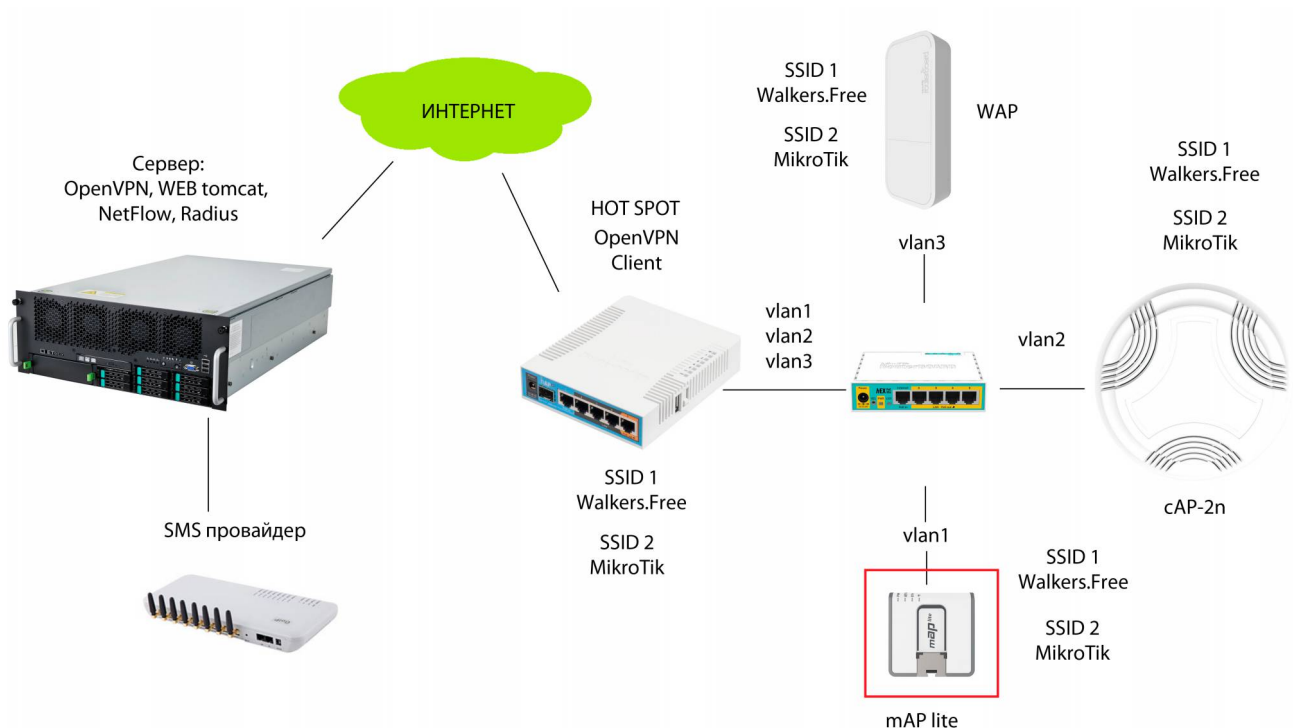


Используем его как свитч и поэтому добавим **ether1-gateway** и группу портов 2-5 в **local-bridge**. Вторым действием можно добавить **vlan1, vlan2, vlan3** с метками

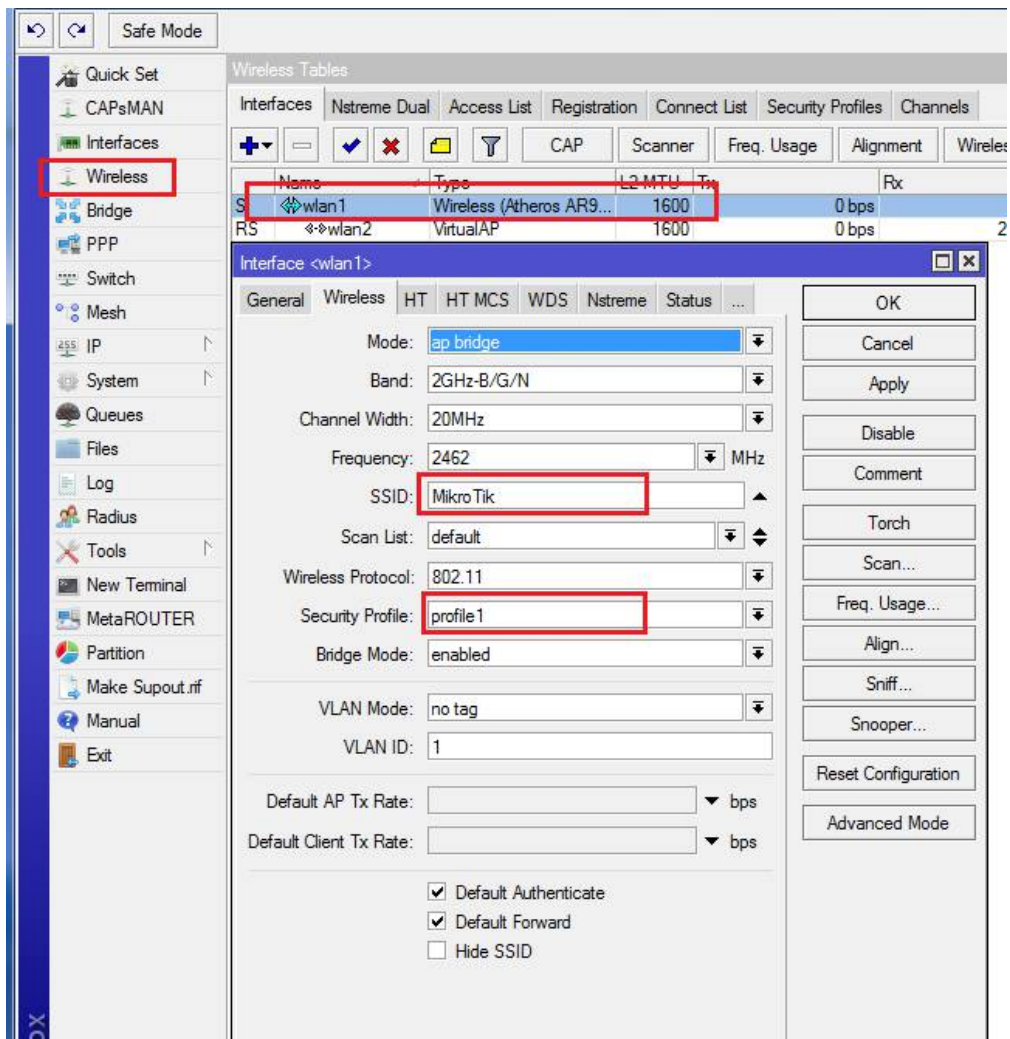
1, 2, 3 прикрепив их к этому бриджу. Дополнительно, если необходимо, можно удалить IP адрес 192.168.88.1/24 с маршрутизатора, выключить DHCP сервер, и навесить DHCP-client на local-bridge:



Далее настроим одну из конечных Wi-Fi точек доступа mAP lite:



Настроим сеть персонала кафе на mAP lite выбрав предварительно созданный **profile1** где содержатся параметры шифрования и пароль доступа к сети:



Создадим виртуальную точку доступа **wlan2** с SSID Walkers. Используем профиль **default** который не содержит пароля. Запрещаем forward клиентам данными между друг другом:

Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles Cha

+ - ✓ ✗ 📄 📡 CAP Scanner Freq. Usage Alignment

Name	Type	L2 MTU	Tx	Rx
wlan1	Wireless (Atheros AR9...	1600		0 bps
wlan2	VirtualAP	1600		0 bps

Interface <wlan2>

General Wireless WDS Status Traffic

SSID: Walkers

Master Interface: wlan1

Security Profile: default

VLAN Mode: no tag

VLAN ID: 1

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

OK Cancel Apply Disable Comment Copy Remove Advanced Mode Torch

enabled running slave

Вешаем **vlan1** с id 1 на **bridge-local**:

Interface List

Interface Ethernet EoIP Tunnel IP Tunnel GRE Tunnel VLAN VRRP Bonding LTE

Name	Type	L2 MTU	Tx	Rx
R bridge-local	Bridge	1598	69.4 kbps	
RS vlan1	VLAN	1594	424 bps	
R bridge1	Bridge	1600	0 bps	
RS ether1	Ethernet	1598	5.6 kbps	
RS ether2	Ethernet	1598	146.0 kbps	
S wlan1	Wireless (Atheros AR9...	1600	0 bps	
S wlan2	VirtualAP	1600	0 bps	

Interface <vlan1>

General Status Traffic

Name: vlan1

Type: VLAN

MTU: 1500

L2 MTU: 1594

MAC Address: 4C:5E:0C:D4:74:79

ARP: enabled

VLAN ID: 1

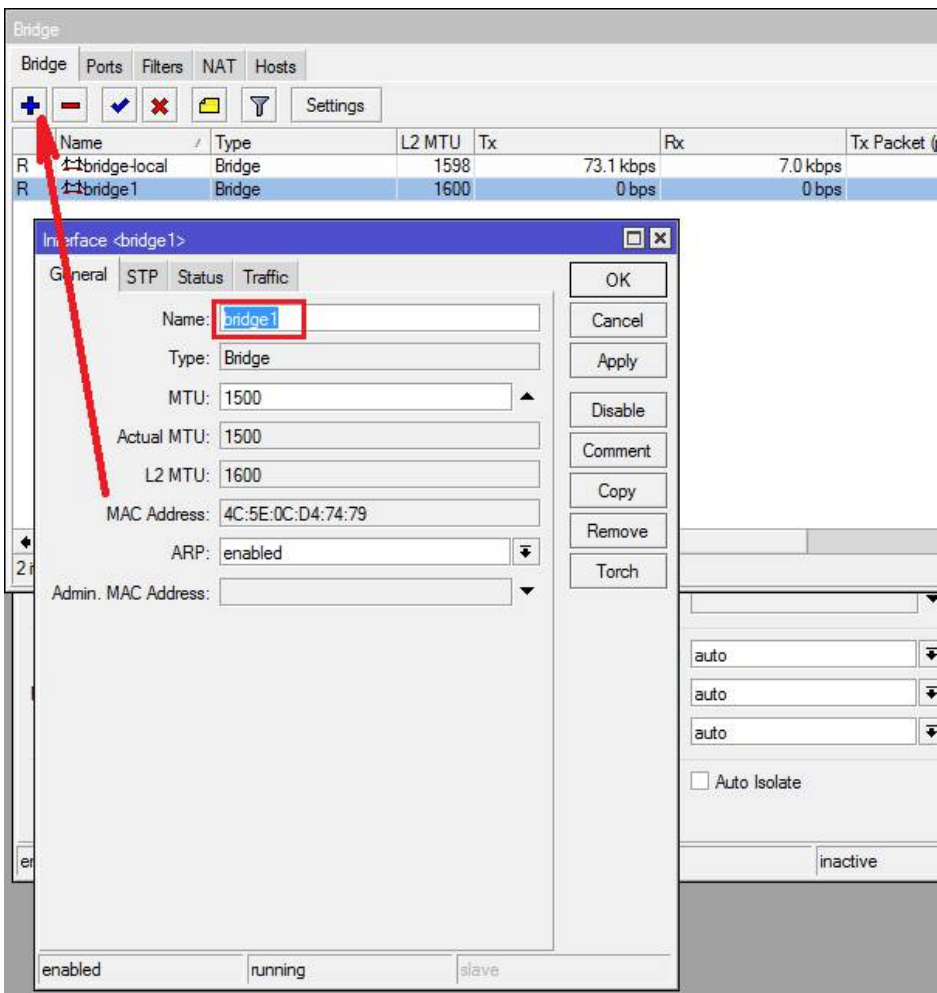
Interface: bridge-local

Use Service Tag

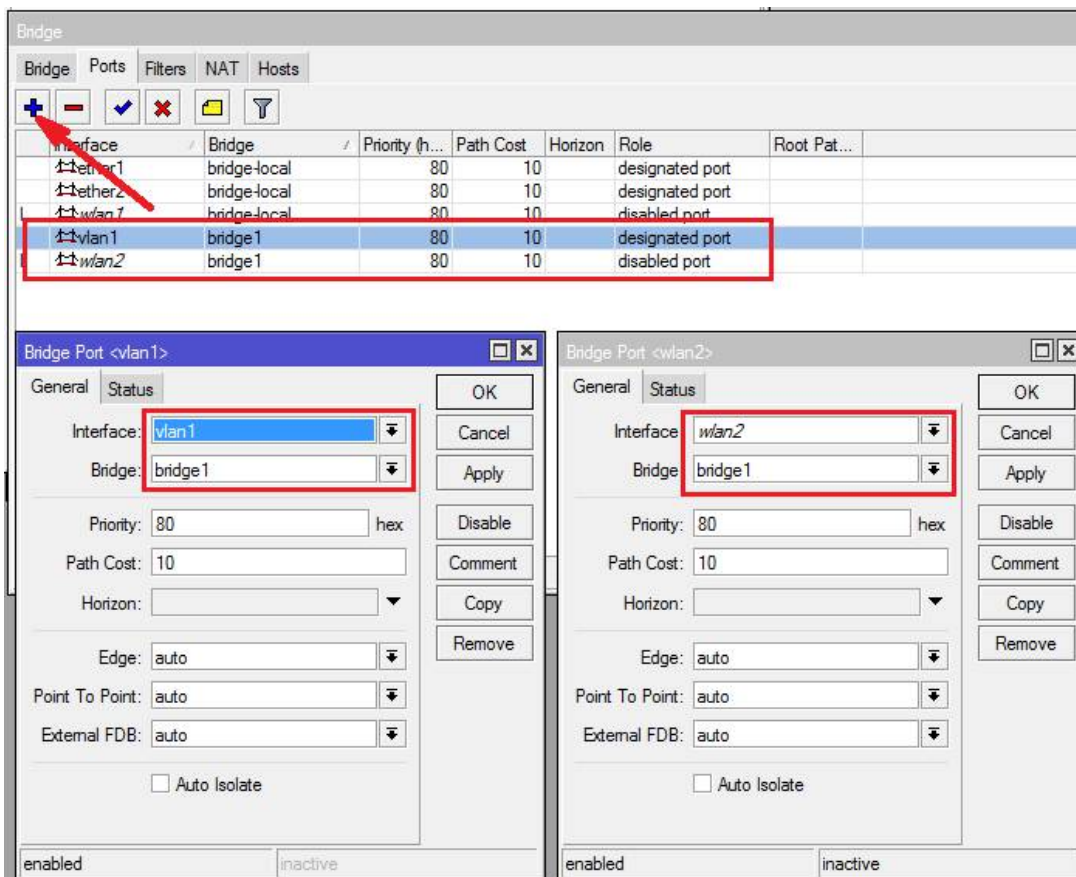
OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave

Создаём новый **bridge1** без настроек:



Добавляем виртуальный локальный интерфейс **vlan1** и виртуальный беспроводной интерфейс **wlan2** (SSID Walkers.Free) в **bridge1**:



Дополнительно по аналогии с hEX PoE lite можно удалить IP адрес 192.168.88.1/24, DHCP сервер, правила фильтрации.

Настройка закончена! Конфигурацию хотспота с SMS авторизацией для nAP-2n можно скачать по этой [ссылке](#). Логин: admin пароля нет.