

Настройка на Микротик контроллера CAPsMAN v2

 mikrotiklab.ru/nastrojka/artga-capsman-v2.html

October 13, 2020



Гвоздём нашей программы будет настройка CAPsMAN v2 на роутере MikroTik – то есть контроллера управления точками доступа. Он позволяет конфигурировать устройства из единого места, назначать каналы и их ширину, SSID, профили безопасности, централизованную блокировку устройств, аутентификация устройств на основе сертификатов, и много другое. Обновлённая версия продукта входит в стандартный пакет RouterOS с версии 6.37. Первой версии не совместима со второй. Для его работы нужен уровень лицензии 4 и выше.

Стоит отметить важный нюанс, если все ваши точки доступа, настроены на получение конфигураций от контроллера, и он по каким-либо причинам не доступен, то все AP прекратят своё вещание до тех пор, пока CAPsMAN не станет доступным.

Содержание

1. [Схема сети](#)
2. [Настройка CAPsMAN](#)
3. [Channels](#)

4. [Datapath](#)
5. [Security](#)
6. [Configurations](#)
7. [Provisioning](#)
8. [Включение CAPsMAN](#)
9. [Настройка AP](#)
10. [Бесшовный роуминг](#)
11. [Настройка сертификатов](#)

Схема сети

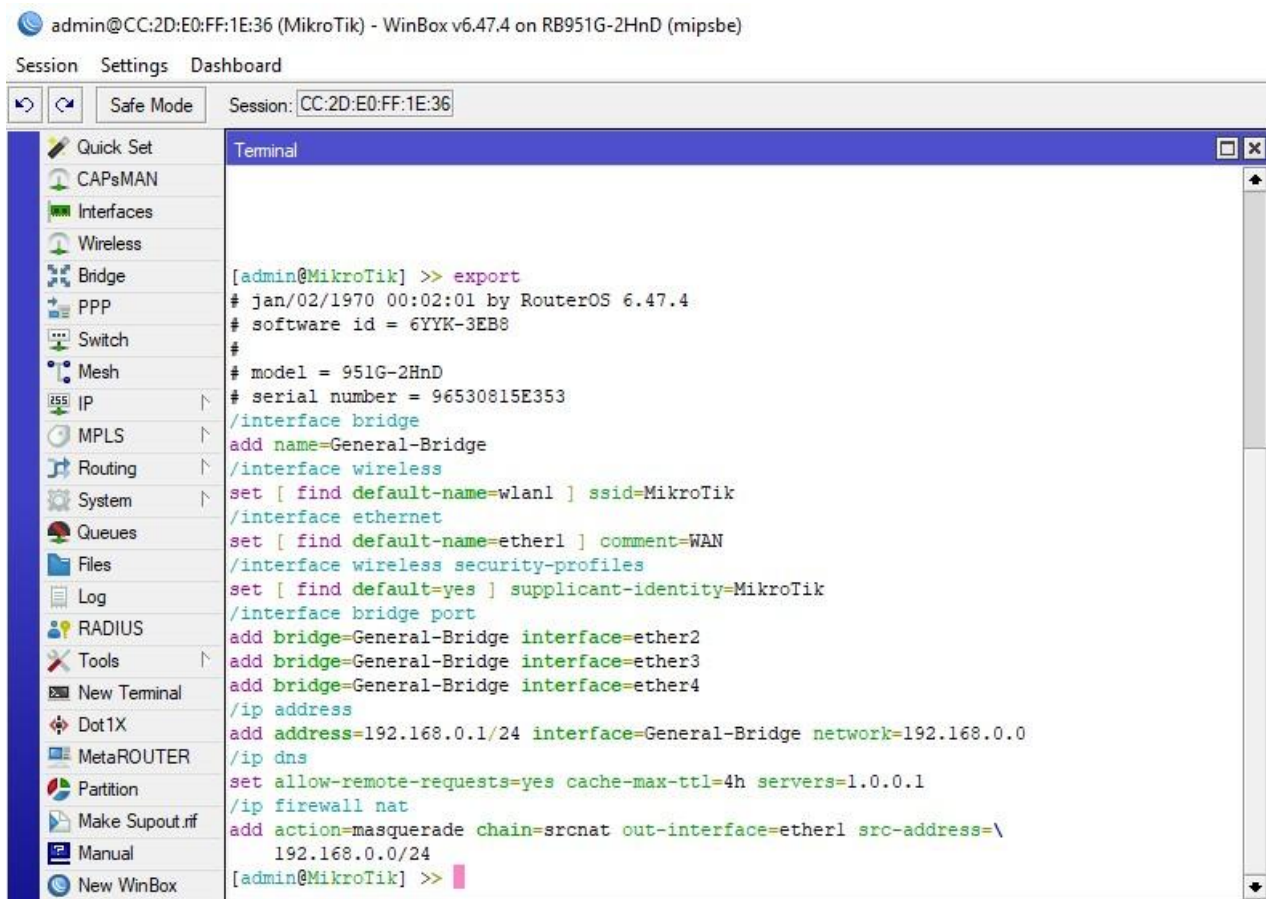
- RouterOS 6.47.4;
- 192.168.0.0/24 – LAN;
- Mikrotik RB951G-2HnD – CAPsMAN, настроен интернет, DNS, DHCP;
- Mikrotik RB951Ui-2HnD и RB951Ui-2nD (hAP) – точки доступа;
- Устройства подключены по кабелю.

Наша команда рекомендует изучить [Наша команда рекомендует изучить углубленный курс по администрированию сетевых устройств MikroTik](#) В курсе много лабораторных работ по итогам которых вы получите обратную связь. После обучения вы получите диплом гос. образца РФ. Подробности и доступ к началу курса бесплатно [здесь](#).

Настройка CAPsMAN

Подключимся на роутер RB951G и выведем действующую конфигурацию:

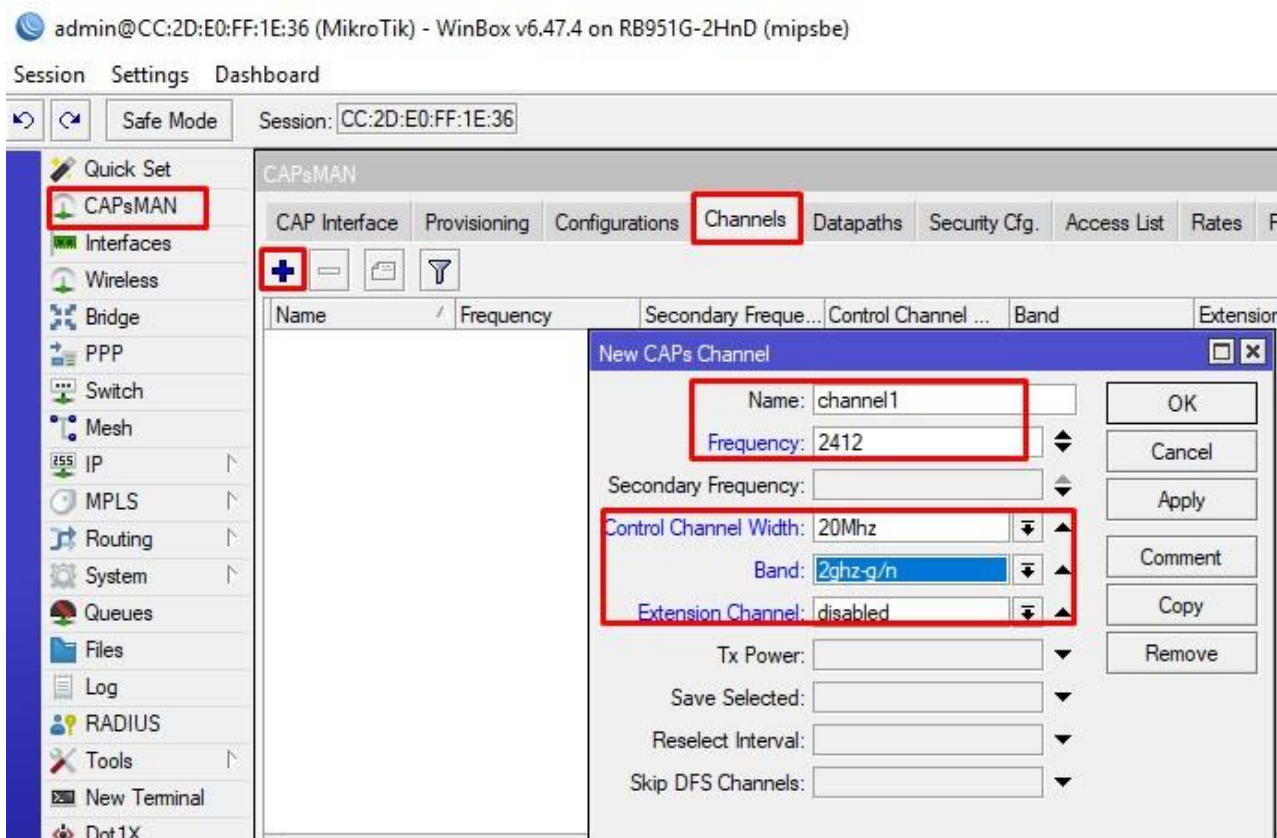
В General-Bridge входят ether2-4, ether1 – смотрит в интернет (выход в интернет у нас отсутствует, т.к. для демонстрации решения он нам не понадобится), назначен IP адрес, DNS и NAT.



Все настройки будут производиться в меню CAPsMAN.

Channels

Создадим первый канал на частоте 2412, ширина в 20Mhz, стандарт G и N.



CAPsMAN

CAP Interface

Provisioning

Configurations

Channels

Datapaths

Security Cfg.

Access List

Rates

Remote CAP

+

—

☰

⌵

Name	Frequency	Secondary Freque...	Control Channel ...	Band	Extension Channel
channel1	2412		20Mhz	2ghz-g/n	disabled
channel6	2437		20Mhz	2ghz-g/n	disabled
channel11	2462		20Mhz	2ghz-g/n	disabled

Datapath

Создадим правило, которое будет добавлять в локальный General-Bridge интерфейсы подключённых AP.

- Local Forwarding – если не установлена галочка, значит клиентская AP будет форвардить трафик через контроллер. Если у вас много точек доступа, от 5-10 и на них много клиентов, то для разгрузки лучше включать данную галочку.
- Client to Client Forwarding – данный параметр разрешает обмениваться трафиком между клиентами AP.



The screenshot shows the CAPsMAN interface with the 'Datapaths' tab selected. A dialog box titled 'New CAPs Datapath Configuration' is open, displaying various configuration options. The 'Name' field is set to 'datapath1'. The 'Bridge' dropdown is set to 'General-Bridge'. The 'Local Forwarding' checkbox is unchecked, and the 'Client To Client Forwarding' checkbox is checked. The 'Datapaths' tab in the main window is highlighted with a red box.

Создадим второй Datapath для гостевой сети. В нем отключим обмен данными между клиентами.

CAPsMAN

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

+ [] [] []

Name	Bridge	L
datapath1	General-Bridge	n

1 item

New CAPs Datapath Configuration

Name:

MTU:

L2 MTU:

ARP:

Bridge:

Bridge Cost:

Bridge Horizon:

Local Forwarding: ☐

Client To Client Forwarding: ☐

VLAN Mode:

VLAN ID:

Interface List:

OK Cancel Apply Comment Copy Remove

Security

Сконфигурируем профиль безопасности для защищённой сети, указав:

- Имя профиля;
- Тип аутентификации;
- Шифрование;
- Пароль.

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

tion Type Encryption Group Encryption Group Key Update Passphrase EAP Methods

New CAPs Security Configuration

Name: security1

Authentication Type: ☐ WPA PSK ☒ WPA2 PSK ☐ WPA EAP ☐ WPA2 EAP ▲

Encryption: ☒ aes ccm ☐ tkip ▲

Group Encryption: ▼

Group Key Update: ▼

Passphrase: ***** ▲

Disable PMKID: ▼

EAP Methods: ▲▼

EAP Radius Accounting: ▼

TLS Mode: ▼

TLS Certificate: ▼

OK Cancel Apply Comment Copy Remove

Настроим второй профиль, для открытой сети, без указания типов шифрования, пароля и т.д.

CAPsMAN

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

+ - [icon] [icon]

Name	Authentication Type	Encryption	Group Encryption	Group Key Update	Passphrase	EAP Methods
security1	WPA2 PSK	aes ccm			*****	
security2						

2 items

CAPs Security Configuration <security2>

Name: security2

Authentication Type: ▼

Encryption: ▼

Group Encryption: ▼

Group Key Update: ▼

Passphrase: ▼

Disable PMKID: ▼

EAP Methods: ▲▼

EAP Radius Accounting: ▼

TLS Mode: ▼

TLS Certificate: ▼

OK Cancel Apply Comment Copy Remove

Configurations

На данном этапе мы создаём конфигурации. Т.к. у нас будет закрытые и открытые сети, то нам понадобятся 2 конфига. Для первого в wireless укажем:

- Имя конфигурации;
- Режим работы;
- SSID;
- Место нахождения;
- Hw. Protection Mode;
- Страна;
- Максимальное количество клиентов.

The screenshot shows the 'New CAPs Configuration' dialog box in the CAPsMAN application. The 'Configurations' tab is selected. The 'Wireless' sub-tab is active. The following fields are filled:

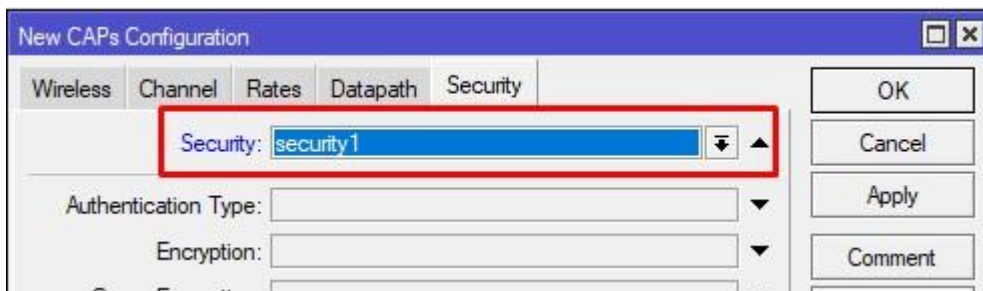
- Name: cfg1
- Mode: ap
- SSID: Wi-Fi-1
- Distance: indoors
- Hw. Protection Mode: cts to self
- Country: russia3
- Max Station Count: 20

A red box highlights the 'Wireless' sub-tab and the fields: Name, Mode, SSID, Distance, Hw. Protection Mode, Country, and Max Station Count.

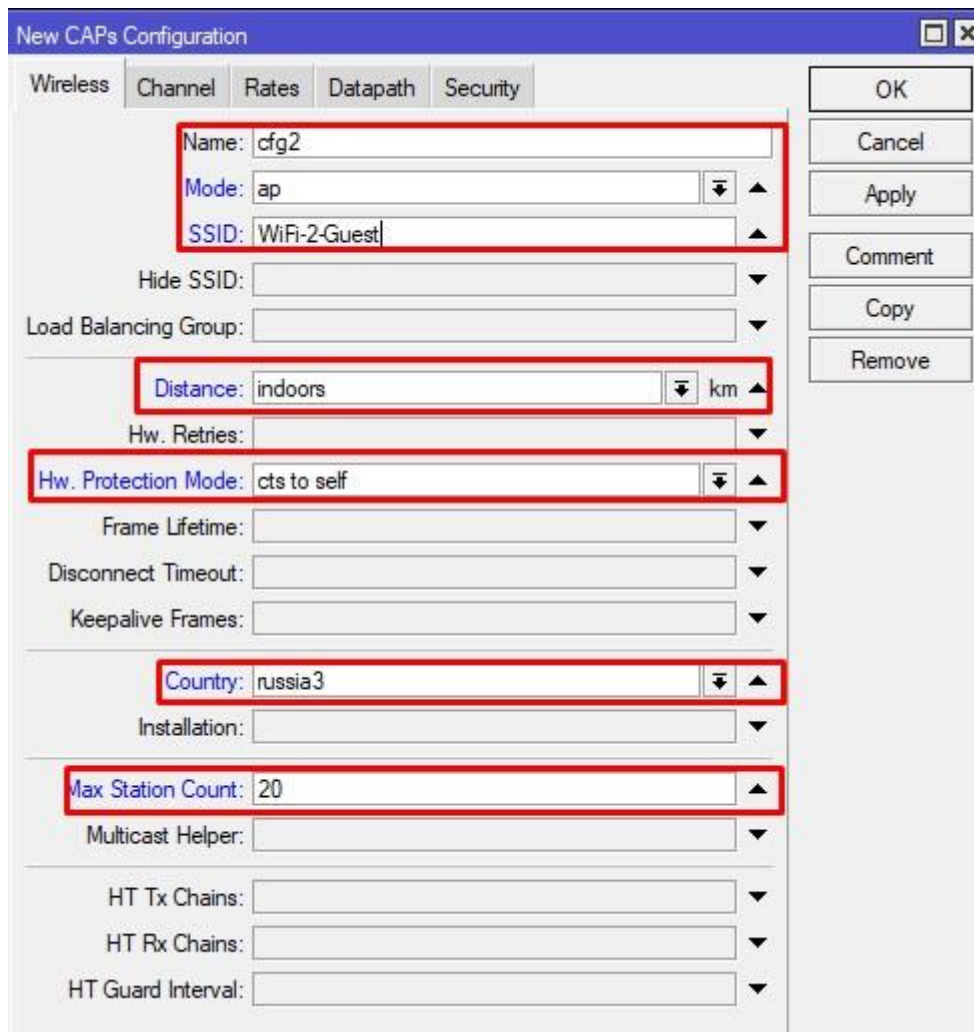
Откроем Datapath и выберем первый.

The screenshot shows the 'New CAPs Configuration' dialog box with the 'Datapath' sub-tab selected. The 'Datapath' dropdown is set to 'datapath1'. A red box highlights the 'Datapath' dropdown.

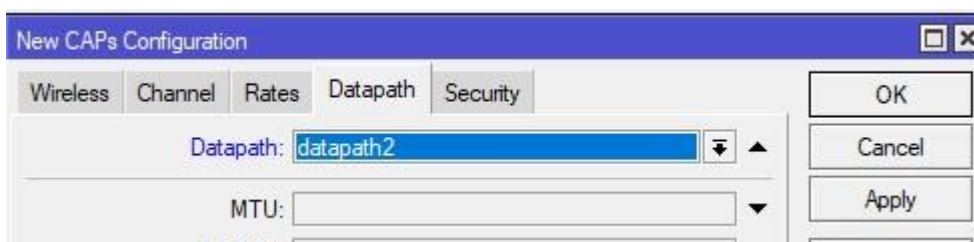
Профиль безопасности так же нужен первый.

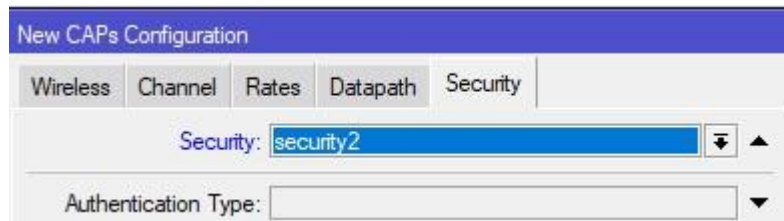


Создадим второй конфиг с незначительными изменениями.



Datapath и Security Profile выберем вторые.





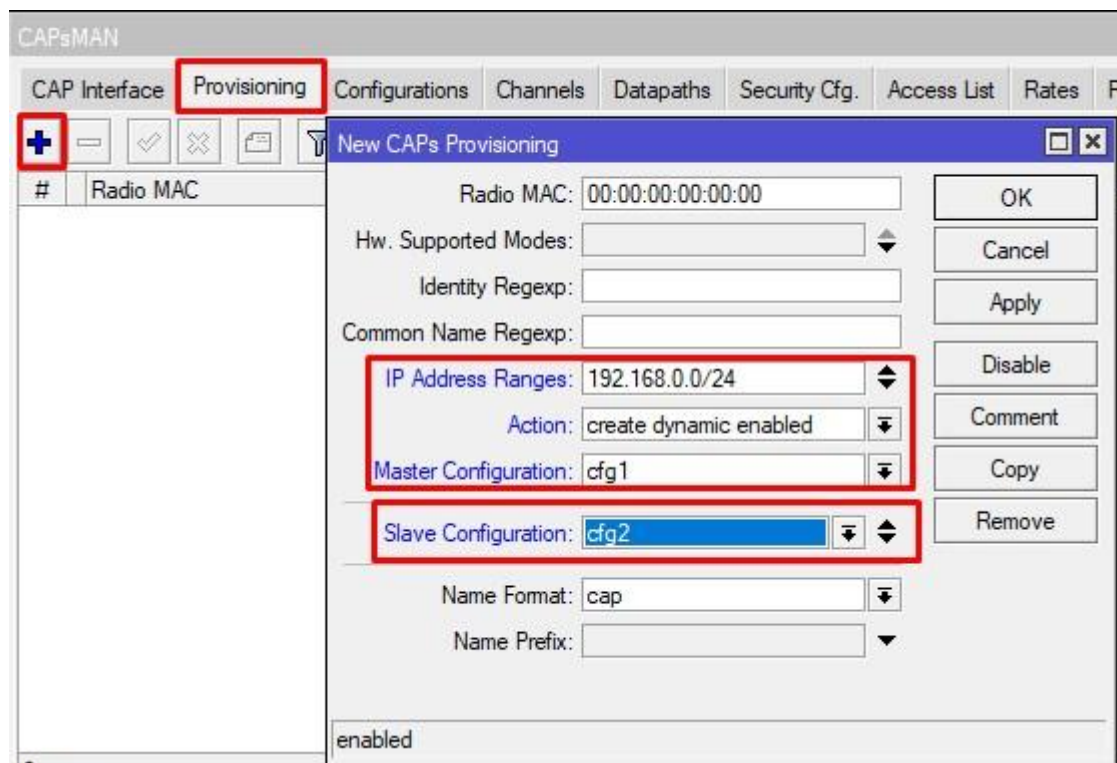
The image shows the 'New CAPs Configuration' dialog box with tabs for Wireless, Channel, Rates, Datapath, and Security. The Security tab is active, showing a dropdown menu for 'Security' set to 'security2' and an empty 'Authentication Type' dropdown.

Provisioning

Задаём параметры для Provisioning. Идентифицировать клиента мы будем по IP адресу, но можно и по имени (System — Identity), а также MAC, но можно и все вместе. Задаём действие – создать динамически и включить, укажем основной и дополнительные конфиги (их может быть до 32-ух, это ограничение RouterOS).

Action могут быть различные:

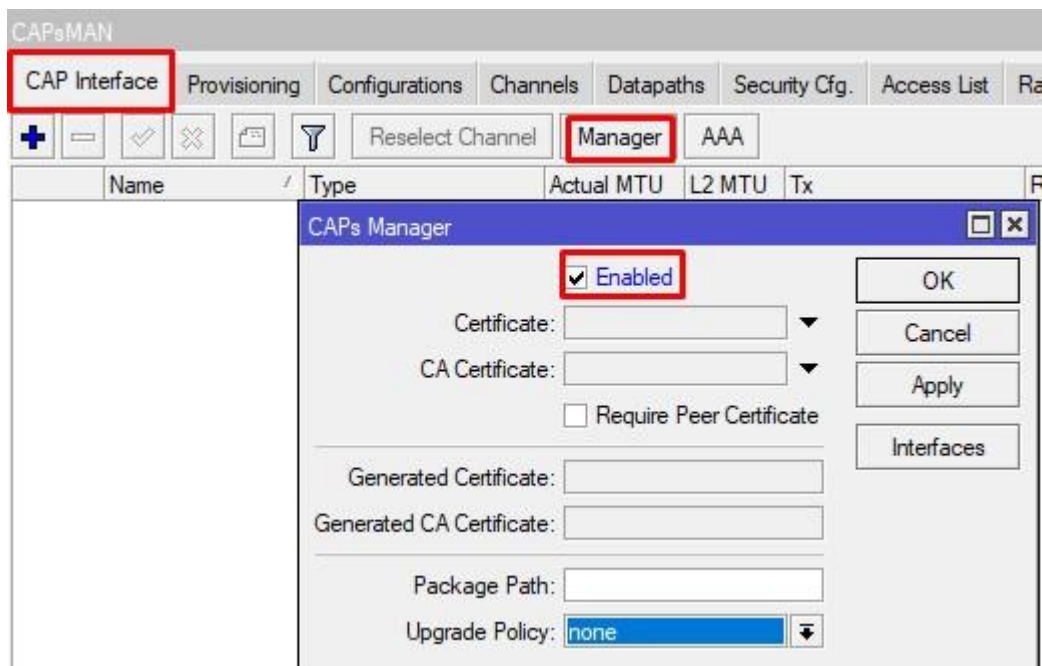
- None – ничего не делать;
- Create enabled – в этом случае создаются статические интерфейсы;
- Create disabled – создать и выключить;
- Create dynamic enabled – используется для тестирования, после чего рекомендуется прибить гвоздями Create enabled.



The image shows the 'CAPsMAN' interface with the 'Provisioning' tab selected. A 'New CAPs Provisioning' dialog box is open. The dialog has fields for 'Radio MAC' (00:00:00:00:00:00), 'Hw. Supported Modes', 'Identity Regexp', 'Common Name Regexp', 'IP Address Ranges' (192.168.0.0/24), 'Action' (create dynamic enabled), 'Master Configuration' (cfg1), 'Slave Configuration' (cfg2), 'Name Format' (cap), and 'Name Prefix'. The 'IP Address Ranges', 'Action', 'Master Configuration', and 'Slave Configuration' fields are highlighted with red boxes. The 'enabled' checkbox at the bottom is checked.

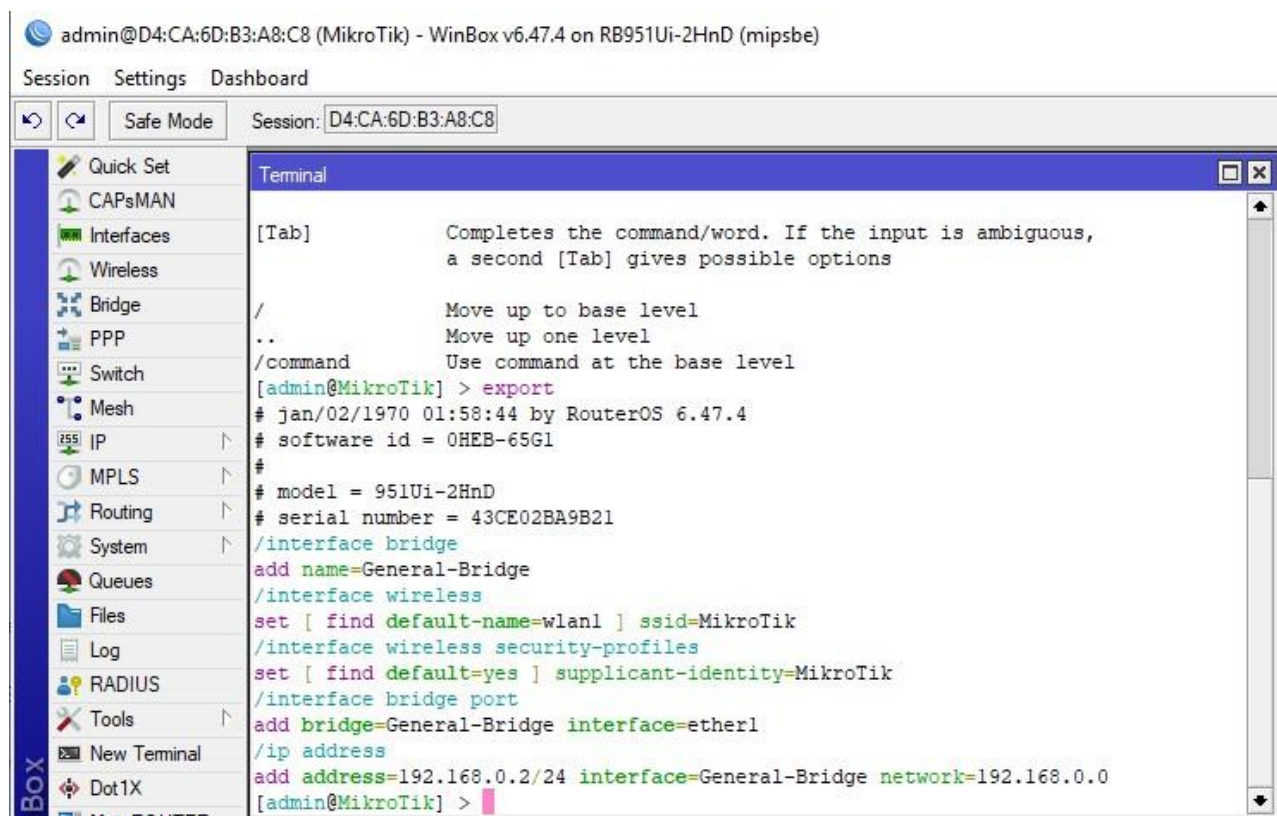
Включение CAPsMAN

Столько мучений, ради одной заветной галочки.



Настройка AP

Подключимся к микротику RB951Ui-2HnD и взглянем на его настройки. Ничего особенного. Имеем бридж и адрес на нем.

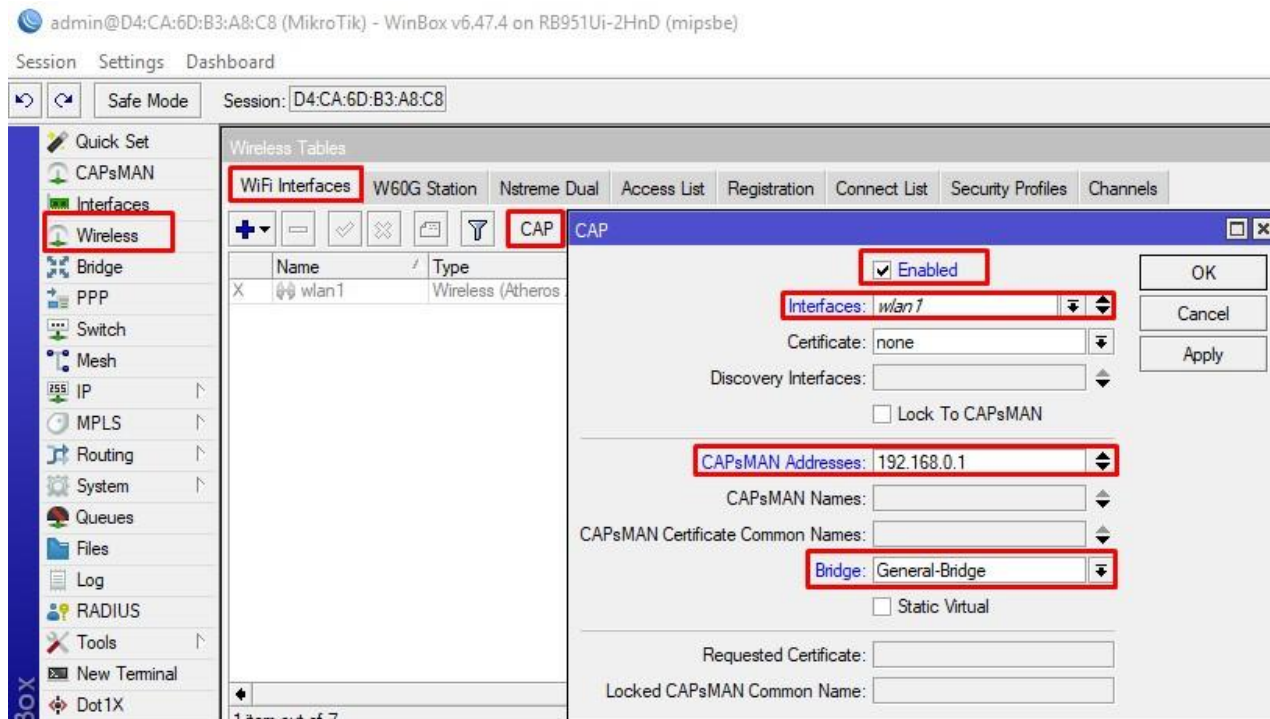


Для получения конфига, перейдём в Wireless – CAP:

- Включаем CAP;
- Interface – тот, на котором будут применены настройки;
- CAPsMAN Address – указываем адрес контроллера, для обеспечения резервации можно указать несколько, если таковы у вас имеются;

- Bridge – тот мост, в который добавятся созданные интерфейсы с полученных конфигураций с контролера.

Обратите внимание, что wlan1 отключён.



В качестве примера, мы добавляем и WiFi-1 и WiFi-2-Guest в общий бридж. В реальной жизни так делать, конечно, не надо. Следует разделить все по VLAN: основной сети, гостевой и management vlan.

Как вы видите, появился соответствующий комментарий, теперь данной AP управляет контроллер.

Wireless Tables					
WiFi Interfaces					
W60G Station Nstreme Dual Access List Registration Connect List Security Profiles Channels					
+ - ✓ ✕ CAP WPS Client Setup Repeater Scanner Freq					
	Name	Type	Actual MTU	Tx	Rx
	--- managed by CAPsMAN				
	--- channel: 2452/20-Ce/gn(17dBm), SSID: WiFi-1, CAPsMAN forwarding				
X	wlan1	Wireless (Atheros AR9...	1500		0 bps
	--- managed by CAPsMAN				
	--- SSID: WiFi-2-Guest, CAPsMAN forwarding				
DX	wlan2	Virtual	1500		0 bps

После того как прилетят настройки, мы их увидим в описании каждого интерфейса. Но внимательный читатель заметит, что конфиг немного не тот, что указывали выше, в частности канал, согласно параметрам нам должен был прилететь 2412, а по факту 2452. Исправим это на контроллере. На вкладке CAP Interface мы видим все успешно подключённые клиентские AP. Флаг D означает – динамический.

CAPsMAN

CAP Interface

Provisioning

Configurations

Channels

Datapaths

Security Cfg.

Access List

Rates

Remote CAP

F

Превратим их в статические и зададим корректные каналы. Двойным кликом открываем cap1, жмём copy.

Interface <cap1>

General

Wireless

Channel

Rates

Datapath

Security

Status

...

Configuration: cfg1

Mode: ap

SSID: WiFi-1

Hide SSID:

Load Balancing Group:

Distance: indoorskm

Hw. Retries:

Hw. Protection Mode: cts to self

OK

Copy

Remove

Torch

Scan...

Reselect Channel

В скопированном интерфейсе указываем корректный канал, datapath, cfg и security.

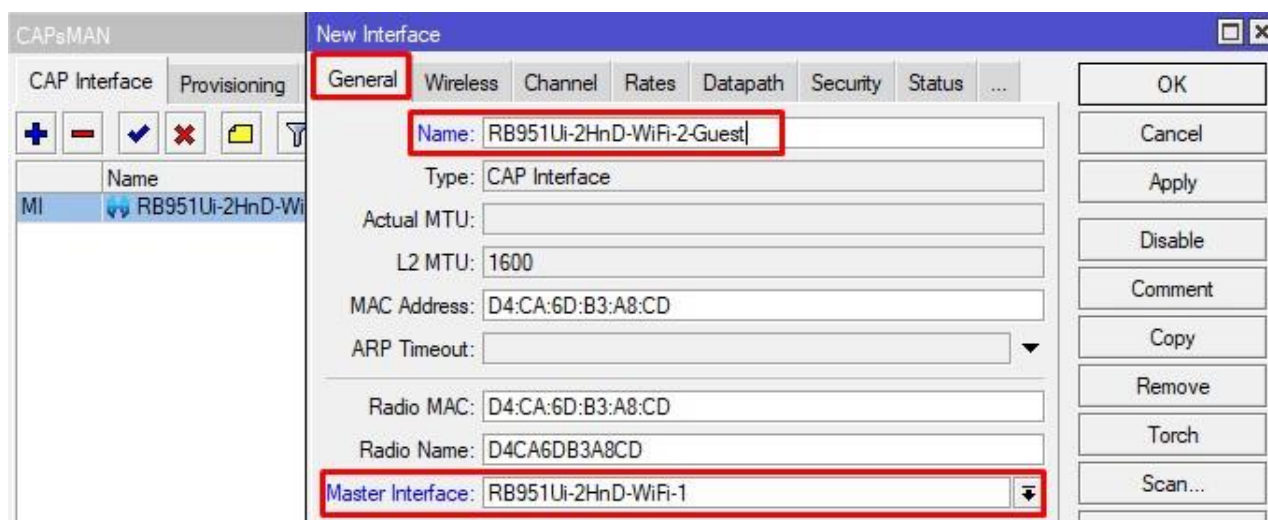
The image shows four sequential screenshots of the 'New Interface' configuration window in MikroTik WinBox. Each screenshot represents a different tab in the configuration process:

- General tab:** The 'Configuration' dropdown is set to 'cfg1'.
- Wireless tab:** The 'Channel' dropdown is set to 'channel1'.
- Datapath tab:** The 'Datapath' dropdown is set to 'datapath1'.
- Security tab:** The 'Security' dropdown is set to 'security1'.

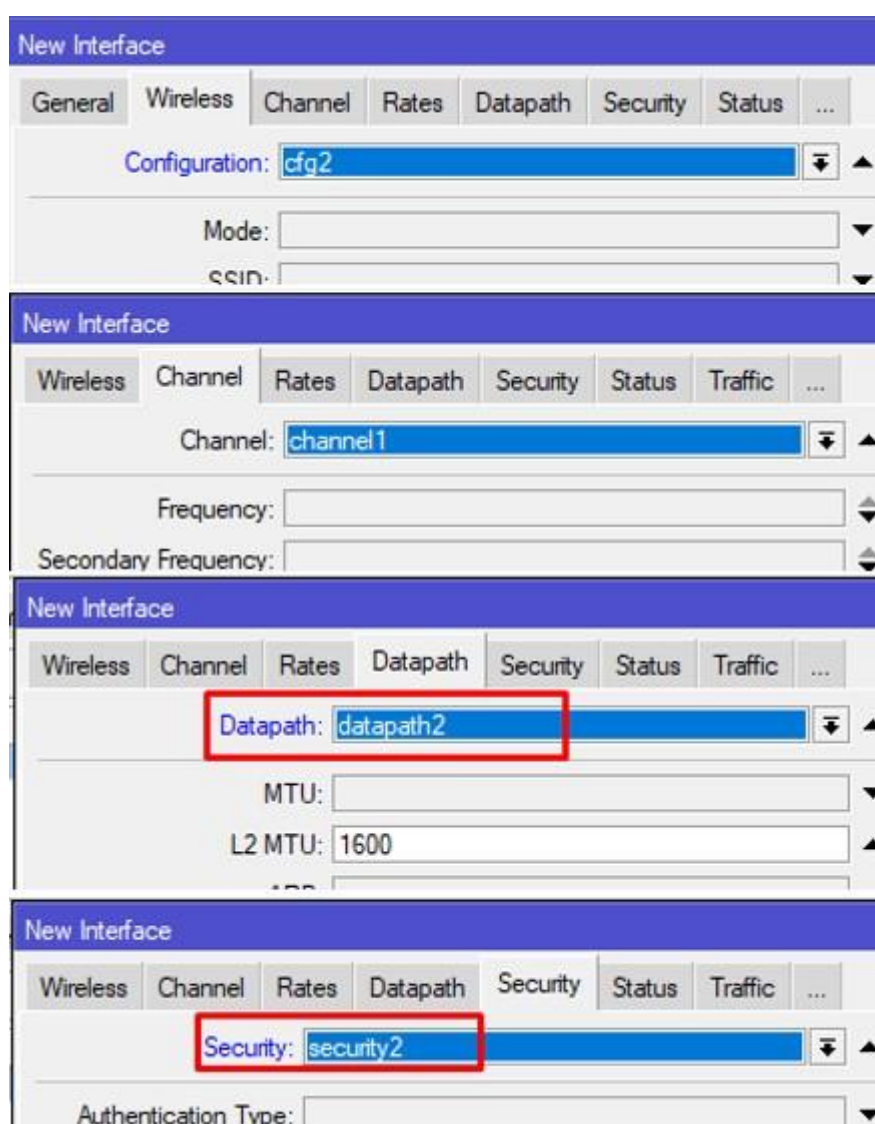
После применения, оба интерфейса пропадут и останется в нашем случае cap3. Переименуем его в понятное имя.

The image shows the 'CAPsMAN' configuration window with the 'Interface <cap3>' dialog open. The 'Name' field is highlighted with a red box and contains the text 'RB951Ui-2HnD-WiFi-1'. The 'Type' is set to 'CAP Interface'. Other fields like 'Actual MTU', 'L2 MTU', and 'MAC Address' are also visible.

После сохранения снова копируем. Задаём корректное имя для WiFi-2-Guest и выбираем Master Interface



Указываем соответствующий конфиг, канал, datapath и профиль безопасности.



Список CAP интерфейсов должен быть следующий.

На клиенте теперь нужно выключить и включить CAP в Wireless. Вот теперь все в порядке.

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths

+ - ✓ ✗ 📄 🔍 Reselect Channel Manager A/

	Name	Type
MI	RB951Ui-2HnD-WiFi-1	CAP Interface
I	RB951Ui-2HnD-WiFi-2-Guest	CAP Interface

admin@D4:CA:6D:B3:A8:C8 (MikroTik) - WinBox v6.47.4 on RB951Ui-2HnD (mipsbe)

Session Settings Dashboard

Safe Mode Session: D4:CA:6D:B3:A8:C8

Quick Set CAPsMAN Interfaces Wireless Bridge PPP Switch Mesh IP MPLS

Wireless Tables

WiFi Interfaces W60G Station Nstreme Dual Access List Registration Conn

+ - ✓ ✗ 📄 🔍 CAP WPS Client Setup Repeater Sca

	Name	Type	Actual MTU	Tx
	--- managed by CAPsMAN			
	--- channel: 2412/20/gn(17dBm), SSID: WiFi-1, CAPsMAN forwarding			
X	wlan1	Wireless (Atheros AR9...	1500	
	--- managed by CAPsMAN			
	--- SSID: WiFi-1, CAPsMAN forwarding			
DX	wlan4	Virtual	1500	

Создадим provisioning для RB951Ui-2nD (hAP) изменив IP Address Ranges, или указав Radio MAC, в качестве эксперимента попробуем этот вариант (в реальной жизни, старайтесь соблюдать единообразие конфигов). Этот тот самый MAC, который светится в настройках конкретной карточки.

New CAPs Provisioning

Radio MAC: CC:2D:E0:6D:9E:37

Hw. Supported Modes:

Identity Regexp:

Common Name Regexp:

IP Address Ranges:

Action: create dynamic enabled

Master Configuration: cfg1

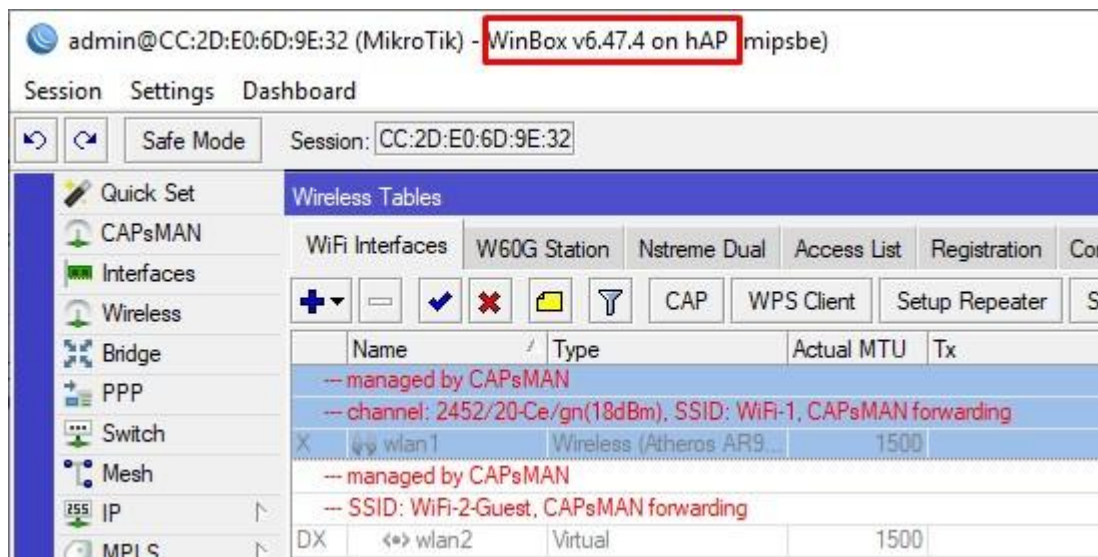
Slave Configuration: cfg2

Name Format: cap

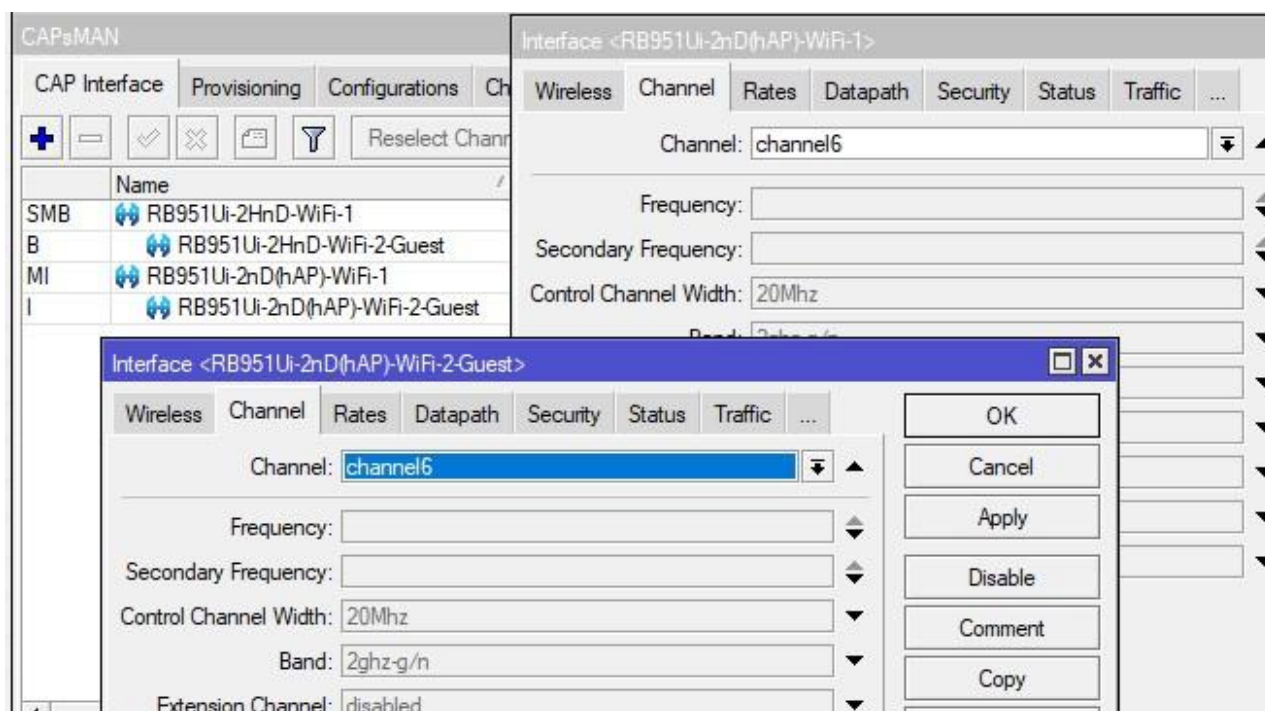
Name Prefix:

OK Cancel Apply Disable Comment Copy Remove

Теперь включим CAP на RB951Ui-2nD (hAP).



Снова проблемы с каналами. Прделаем такой же трюк с копированием интерфейсов, необходимо изменить частоту согласно channel6. Не забываем про профили безопасности, datapath и cfg.



После выключения/включения CAP, должны получить правильный конфиг.

admin@CC:2D:E0:6D:9E:32 (MikroTik) - WinBox v6.47.4 on hAP (mipsbe)

Session Settings Dashboard

Safe Mode Session: CC:2D:E0:6D:9E:32

Quick Set CAPsMAN Interfaces Wireless Bridge PPP Switch Mesh IP MPLS

Wireless Tables

WiFi Interfaces W60G Station Nstreme Dual Access List Registration Connect Li

+ - ✓ ✗ 📁 🔍 CAP WPS Client Setup Repeater Scanner

Name	Type	Actual MTU	Tx
--- managed by CAPsMAN			
--- channel: 2437/20/gn(18dBm), SSID: WiFi-1, CAPsMAN forwarding			
X wlan1	Wireless (Atheros AR9...	1500	0 bps
--- managed by CAPsMAN			
--- SSID: WiFi-2-Guest, CAPsMAN forwarding			
DX wlan3	Virtual	1500	0 bps

У нас остался третий девайс, это сам контроллер. Да-да, он может быть так же сам для себя им.

admin@CC:2D:E0:FF:1E:36 (MikroTik) - WinBox v6.47.4 on RB951G-2HnD (mipsbe)

Session Settings Dashboard

Safe Mode Session: CC:2D:E0:FF:1E:36

Quick Set CAPsMAN Interfaces Wireless Bridge PPP Switch Mesh IP MPLS Routing System Queues Files Log RADIUS Tools New Terminal Dot1X MetaROUTER

CAPsMAN

CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access

+ - ✓ ✗ 📁 🔍 Reselect Channel Manager AAA

Name	Type	Actual MTU	L2 M
SMB RB951G-2HnD-WiFi-1	CAP Interface	1500	1
B RB951G-2HnD-WiFi-2-Guest	CAP Interface	1500	1
SMB RB951Ui-2HnD-WiFi-1	CAP Interface	1500	1
B RB951Ui-2HnD-WiFi-2-Guest	CAP Interface	1500	1
SMB RB951Ui-2nD(hAP)-WiFi-1	CAP Interface	1500	1
B RB951Ui-2nD(hAP)-WiFi-2-Guest	CAP Interface	1500	1

Wireless Tables

WiFi Interfaces W60G Station Nstreme Dual Access List Registration Connect List Se

+ - ✓ ✗ 📁 🔍 CAP WPS Client Setup Repeater Scanner Fre

Name	Type	Actual MTU	Tx	Rx
--- managed by CAPsMAN				
--- channel: 2462/20/gn(17dBm), SSID: WiFi-1, CAPsMAN forwarding				
X wlan1	Wireless (Atheros AR9...	1500	0 bps	
--- managed by CAPsMAN				
--- SSID: WiFi-2-Guest, CAPsMAN forwarding				
DX wlan3	Virtual	1500	0 bps	

Итого у нас есть 3 девайса, на разных каналах, на каждом по 2 AP с разным SSID. Проверим это!

Scanner									
Interface: wlan1						Start			
<input checked="" type="checkbox"/> Background Scan						Stop			
						Close			
						Connect			
						New Window			
	Address	SSID	Channel	Signal	Noise	Signal	Radio Name	RouterO	
AP	70:F8:2B:73:63:84	Beeline_2G_F17937	2422/2...	-87	0	0			
AP	10:7B:EF:56:AC:38	Keenetic-5236	2422/2...	-93	0	0			
AP	50:FF:20:10:03:48	Keenetic-8932	2447/2...	-89	0	0			
AP	08:C6:B3:BE:D1:12	MTSRouter_192422	2447/2...	-71	0	0			
AP	F0:B4:D2:D0:D9:50	MTSRouter_237188	2472/2...	-87	0	0			
AP	F0:B4:D2:CF:4D:D0	MTS_Router_238373-4dcd	2412/2...	-72	0	0			
AP	BC:0F:9A:0C:1A:1B	MTS_Router_264823-	2472/2...	-87	0	0			
AP	EC:4C:4D:D6:1F:7A	RT-WiFi-1F79	2422/2...	-91	0	0			
APR	D4:CA:6D:B3:A8:...	WiFi-1	2412/2...	-63	0	0	D4CA6DB3A8CD	6.47.4	
APR	CC:2D:E0:6D:9E:37	WiFi-1	2437/2...	-60	0	0	CC2DE06D9E37	6.47.4	
APR	CC:2D:E0:FF:1E:38	WiFi-1	2462/2...	-66	0	0	CC2DE0FF1E38	6.47.4	
AR	D4:CA:6D:B3:A8:...	WiFi-2-Guest	2412/2...	-63	0	0	D4CA6DB3A8CD	6.47.4	
AR	CC:2D:E0:6D:9E:37	WiFi-2-Guest	2437/2...	-61	0	0	CC2DE06D9E37	6.47.4	
AR	CC:2D:E0:FF:1E:38	WiFi-2-Guest	2462/2...	-65	0	0	CC2DE0FF1E38	6.47.4	

Бесшовный роуминг

Интернет пестрит громкими фразами вида «настройка бесшовного wifi (роуминг) на микротик», но чудес не бывает, и это на самом деле псевдо бесшовный роуминг. Для бесшовности в прямом смысле этого слова, вам понадобится протокол 802.11R, реализация которого отсутствует на устройствах Mikrotik, его поддерживают другие более дорогие устройства. Куча манов ведут к «тонкой настройке» Access List путём принудительного выбрасывания с точки при определённом уровне сигнала. Так вот, это абсолютно бессмысленно, т.к. при выкидывании с точки вы лишаетесь того самого псевдо роуминга.

Хитрость состоит в том, что нужно грамотно расставить точки доступа. Под грамотно, я понимаю, чтобы уровень сигнала клиентского устройства был в пределах -70-75 и тогда, CAPsMAN увидит, на основе своего анализа, что у вас блин хреновый сигнал, и переключит на ближайшую точку (если она установлена правильно, если сигнал ее лучше и если она вообще есть). Переключение в ДАННОМ случае, будет начинаться со второго этапа аутентификации, а не с первого, т.е. полного, как ели бы вы сделали это выкидыванием клиентов. Это и есть дополнительная, подчёркиваю, дополнительная фишка, а не крутая реализация роуминга.

Access List нужен для других целей – блокировка / разрешение доступа к точкам. В контексте CAPsMAN это работает централизованно.

CAPsMAN

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

+ - ✓ ✗ 📁 🏠

#	MAC Address	MAC Mask	Interface	Signal Ra...	Action	Client To Clie...	VLAN Mo...	VLAN I
0 items								

New CAPs Access Rule

MAC Address:

MAC Mask:

Interface:

SSID Regexp:

Signal Range:

Allow Signal Out Of Range:

Time:

Action:

AP Tx Limit:

Client Tx Limit:

Private Passphrase:

Client To Client Forwarding:

RADIUS Accounting:

VLAN Mode:

VLAN ID:

OK Cancel Apply Disable Comment Copy Remove

Вы только посмотрите, можно запрещать или разрешать определённым MAC адресам цепляться на конкретных или всех AP.

Начал одним, а закончил другим))), надеюсь теперь все стало понятно.

Настройка сертификатов

К сожалению, первая версия имела изъяны, и без труда можно было прикинуться AP. Ситуация изменилась с появлением сертификатов и улучшенных механизмов работы. Не будем заострять внимание на генерации сертификатов, это, пожалуй, отдельная тема, тем более их можно создавать, не отходя от кассы. Но имейте в виду, что они сгенерятся на максимально возможный срок.

Открываем Manager, в Certificate и CA Certificate ставим значение auto.

Session Settings Dashboard

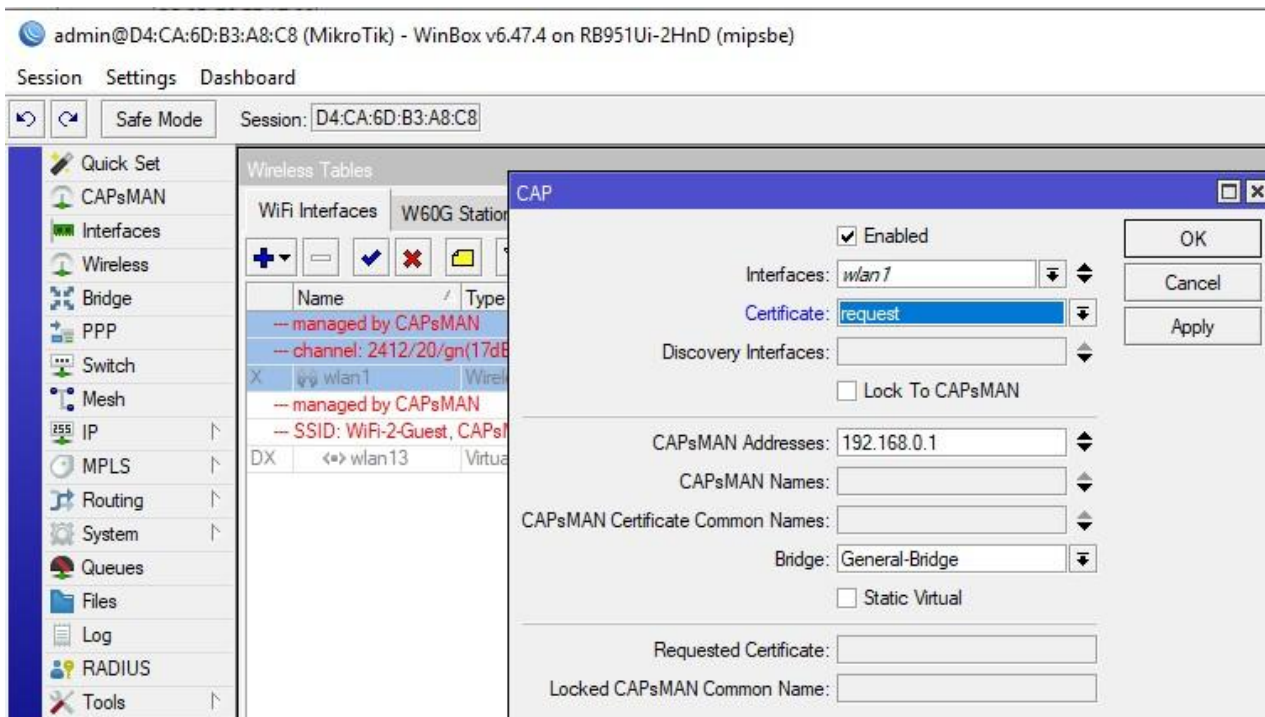
Safe Mode Session: CC:2D:E0:FF:1E:36

The screenshot shows the Mikrotik WinBox interface. On the left is a sidebar with navigation options like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, RADIUS, and Tools. The main window displays the CAPsMAN configuration. The 'CAP Interface' tab is active, showing a table of interfaces. A 'CAPs Manager' dialog box is open, with the 'Enabled' checkbox checked. The 'Certificate' and 'CA Certificate' dropdown menus are both set to 'auto'. The 'Require Peer Certificate' checkbox is unchecked. There are fields for 'Generated Certificate' and 'Generated CA Certificate', and a 'Package Path' field. The 'Upgrade Policy' is set to 'none'. Buttons for 'OK', 'Cancel', 'Apply', and 'Interfaces' are on the right.

После применения, роутер сгенерировал CA и сертификат для роутера. Укажем их вместо auto в выпадающем списке.

This screenshot shows the same CAPsMAN configuration after the certificates have been generated. The 'CAPs Manager' dialog box now shows the 'Certificate' and 'CA Certificate' dropdown menus updated with the generated certificate IDs: 'CAPsMAN-CC2DE0FF1E33' and 'CAPsMAN-CA-CC2DE0FF1E33' respectively. The 'Generated Certificate' and 'Generated CA Certificate' text fields also display these IDs. The 'Enabled' checkbox remains checked, and 'Require Peer Certificate' is still unchecked. The 'Package Path' and 'Upgrade Policy' fields remain unchanged.

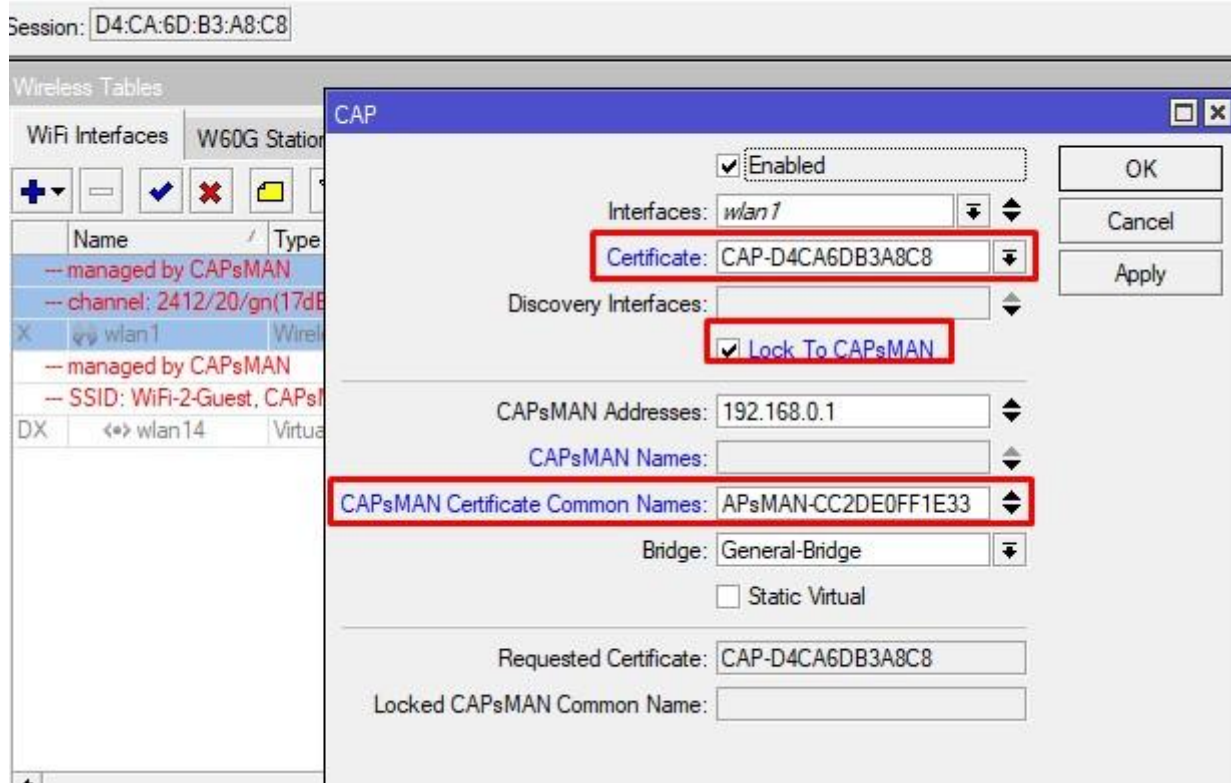
Подключаемся к Mikrotik RB951Ui-2HnD, открываем CAPsMAN в Wireless, в строке Certificate выбираем auto.



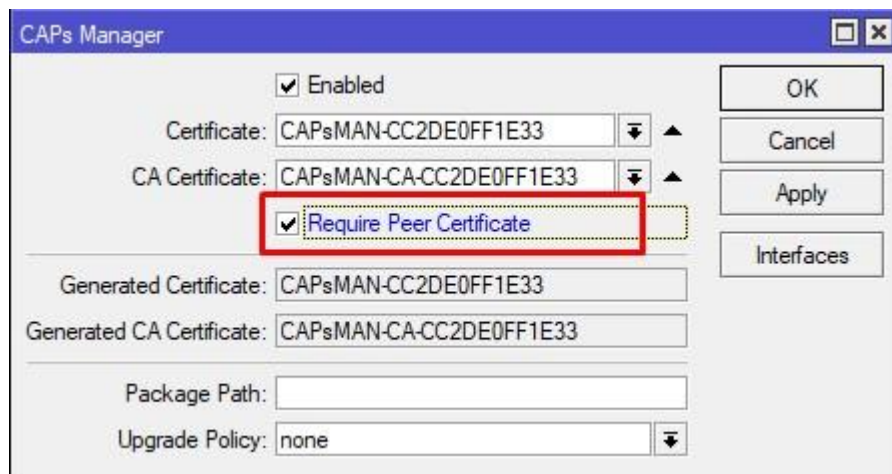
После чего, клиент отправит на контроллер запрос сертификата и получит его. Следом меняем auto на выданный сертификат из выпадающего списка. Так же рекомендую указать CAPsMAN Certificate Common Name. Ставя галочку Lock To CAPsMAN, мы жёстко привязываемся. Но если вы отзовёте сертификат контроллера, то точки перестанут работать.

A8:C8 (MikroTik) - WinBox v6.47.4 on RB951Ui-2HnD (mipsbe)

board



Если все хорошо, то конфиг прилетит без проблем. Проделываем то же самое для остальных AP. После чего на контроллере ставим галочку Require Peer Certificate.



Теперь принудительно требуем у точек наличие сертификата.

Чтобы не городить все в один или разные бриджи, прочтите нашу статью [«Настройка VLAN на микротиках»](#) для красивого разрезания сетей на VLAN.

Удачных конфигов.

Вы хорошо разбираетесь в Микротиках? Или впервые недавно столкнулись с этим оборудованием и не знаете, с какой стороны к нему подступиться? В обоих случаях вы найдете для себя полезную информацию в углубленном курсе [«Администрирование сетевых устройств MikroTik»](#). В курсе много практических лабораторных работ по результату выполнения которых вы получите обратную связь. После окончания обучения вы получите диплом гос. образца РФ. Подробности и доступ к началу курса бесплатно [тут](#).