

# Настройка контроллера CAPsMAN (бесшовный Wi-Fi роуминг) на Mikrotik

 [interface31.ru/tech\\_it/2020/10/nastroyka-kontrollera-capsman-na-mikrotik.html](https://interface31.ru/tech_it/2020/10/nastroyka-kontrollera-capsman-na-mikrotik.html)

## Записки IT специалиста

Технический блог специалистов ООО "Интерфейс"

- [Главная](#)
- Настройка контроллера CAPsMAN (бесшовный Wi-Fi роуминг) на Mikrotik

Во всех случаях, когда вам требуется качественное беспроводное покрытие достаточно большой площади, когда одной точкой доступа не обойтись, встает вопрос роуминга - а именно передачи клиента от одной точки доступа к другой. Желательно сделать этот процесс максимально простым и прозрачным для клиента, без разрыва связи и переподключения, а еще желательно не разориться при выполнении этой задачи. В этом нам поможет оборудование Mikrotik и программный контроллер беспроводной сети CAPsMAN.



### Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на [углубленном курсе по администрированию MikroTik](#). Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.

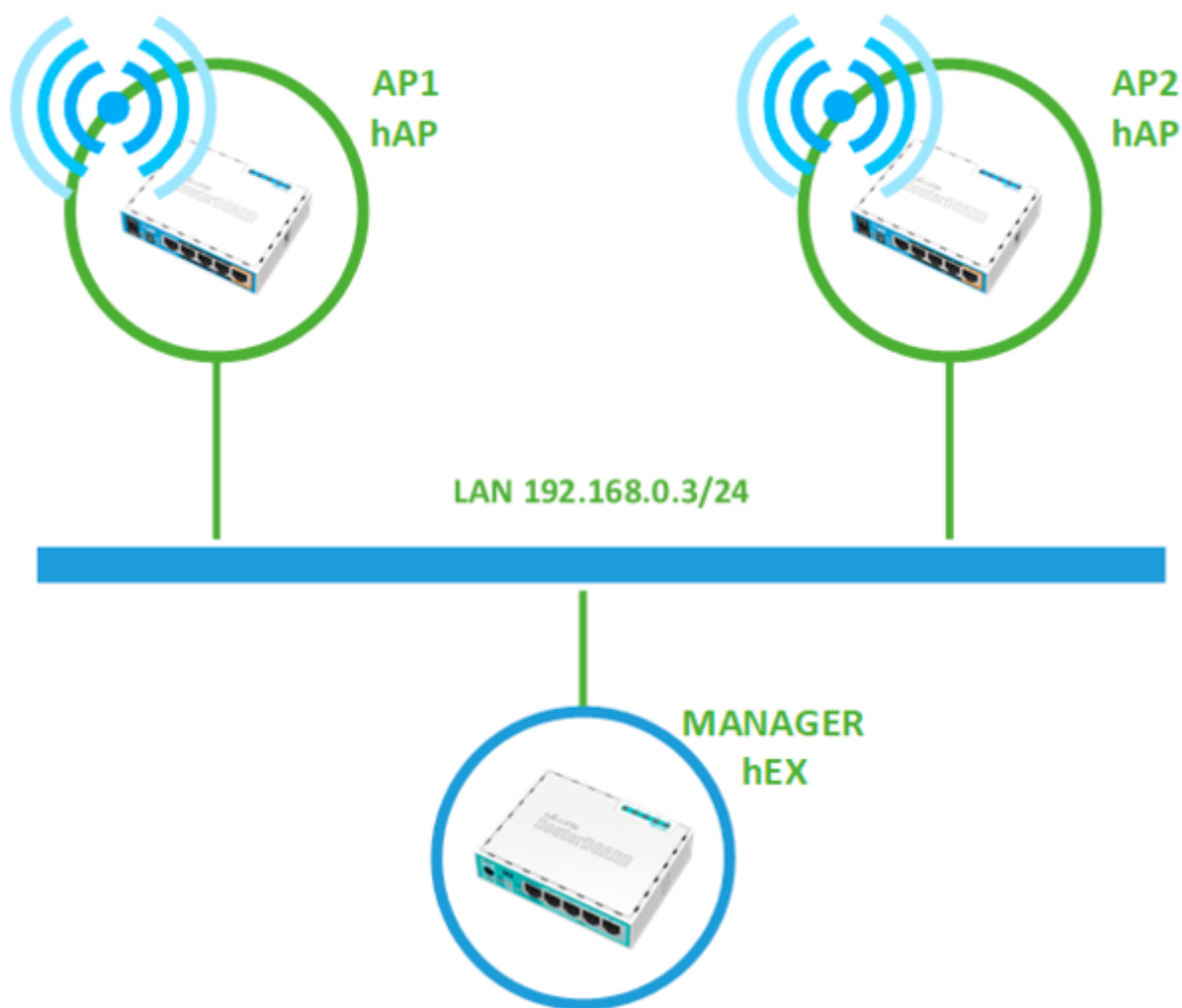
У некоторых читателей сразу может возникнуть вопрос - а почему нельзя просто купить и наставить недорогих точек доступа, настроив на каждой один и тот же SSID и пароль? Сделать так, конечно же можно, только вот такая сеть не будет управляемой и приемлемого качества связи в ней достигнуть будет трудно. Основная проблема в том, что параметрами соединения **всегда управляет клиент** и он может держаться за более далекую и слабую точку до самого конца, хотя рядом есть другая, с более лучшими условиями приема. Получается что вроде бы и покрытие есть и сигнал везде вроде бы хороший, а качество связи оставляет желать лучшего.

Управляемые беспроводные сети работают иначе. Контроллер оценивает взаимное расположение клиента и точек доступа и когда он переходит в область обслуживаемую другой точкой доступа, старая точка его просто отключает, после чего он переподключается к новой, более мощной точке. Это довольно упрощенное изложение, но вполне достаточное для понимания происходящих процессов.

Сразу внесем ясность, настоящим *бесшовным* роумингом это не является, более правильно это назвать быстрым переключением, часть пакетов, особенно если это был поток UDP, при этом неизбежно потеряется. Но будем честными - бесшовный роуминг предполагает оборудование совсем иного класса и стоимости. А большинство современных сетевых приложений, в том числе и голосовые мессенджеры (Skype, Viber и т.д.) вполне нормально переносят быстрое переподключение, пользователь скорее всего даже ничего не заметит.

Но термин *бесшовный* давно устоялся и используется для таких сетей, хотя мы бы назвали его *псевдобесшовным*, но вы должны иметь представление о том, как все обстоит на самом деле и не питать необоснованных иллюзий.

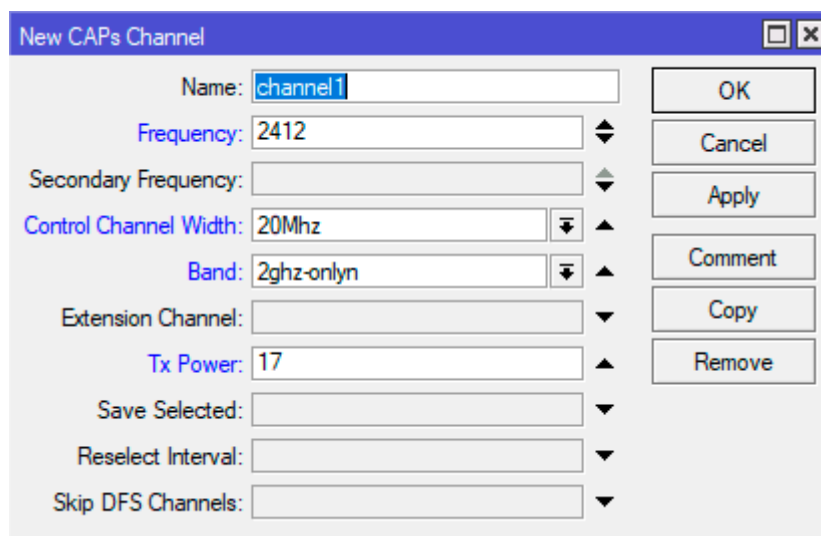
Схема построения псевдобесшовной сети - это беспроводная поверх проводной. В качестве точек доступа вы можете использовать любые точки доступа или иные беспроводные устройства Mikrotik, которые могут работать в таком режиме. Контроллером CAPsMAN может быть любое устройство Mikrotik, даже не имеющее беспроводного интерфейса. В нашем примере мы собрали тестовую схему из двух беспроводных роутеров hAP, выполняющих роль точек доступа и роутера hEX, выступающего в роли контроллера.



Настройку следует начинать с контроллера. Откроем Winbox и перейдем в раздел **CAPsMAN**, здесь нам следует создать ряд необходимых шаблонов, из которых потом, как из кирпичиков, мы будем формировать конфигурации для беспроводных устройств. Мы не будем подробно рассматривать беспроводные настройки, обходясь необходимым минимумом, более подробно об этом вы можете прочитать в нашей статье: [Расширенная настройка Wi-Fi на роутерах Mikrotik. Режим точки доступа](#).

Начнем с рабочих каналов, переходим в **CAPsMAN - Channels** и создаем новую настройку. В самом простом варианте это будет одна рабочая частота, например, **2412 МГц** или **1 канал**. Обратите внимание, выпадающего списка частот тут нет, просто указываем значения руками. Затем задаем ширину канала в поле **Control Channel Width**, если вы указали широкий канал, то укажите и направление его расширения по частоте в поле **Extension Channel**, если мы говорим о первом канале, то здесь единственным значением будет **Ce**, либо можете указать **XX** для автоматического выбора.

В поле **Band** указываем необходимые стандарты работы сети, а в поле **Tx. Power** - мощность передатчика с учетом коэффициента усиления антенн, для hAP это значение равно 17 дБм.



Можно поступить и несколько иначе, не указывать рабочую частоту вообще, в этом случае точки будут выбирать ее автоматически, исходя из эфирной обстановки. В этом случае дополнительно ставим флаг **Save Selected**, что предписывает точке запоминать последнюю выбранную частоту и **Reselect Interval** - интервал времени с периодичностью которого точка будет анализировать эфир и выбирать рабочую частоту.

Еще один вариант - задать список частот доступных точке для выбора, скажем 1 - 6 -11 каналы:

Как лучше сделать? Единственно верного ответа на этот вопрос нет, все зависит от топологии вашей сети и эфирной обстановки. Частотное планирование беспроводных сетей - обширный вопрос, заслуживающий отдельной статьи. Если же коротко, то в том хаосе, что творится в многоквартирных домах и офисных центрах оптимальным решением будет автоматический выбор частоты по всему диапазону, либо из заданного списка. В сетях с небольшим количеством клиентов и достаточным разнесением точек друг от друга можно оставить их все на одной частоте, возникающие при этом коллизии (внутриканальные помехи) протокол достаточно хорошо разрешает. В иных случаях чередуем точки на непересекающихся каналах, к этому мы еще вернемся позже.

Если вы используете оборудование для обоих диапазонов - 2,4 ГГц и 5 ГГц, то создайте настройки каналов для обоих. Также никто вас не ограничивает в их количестве. Можете сразу создать все необходимые варианты, а потом быстро их применять к текущим конфигурациям.

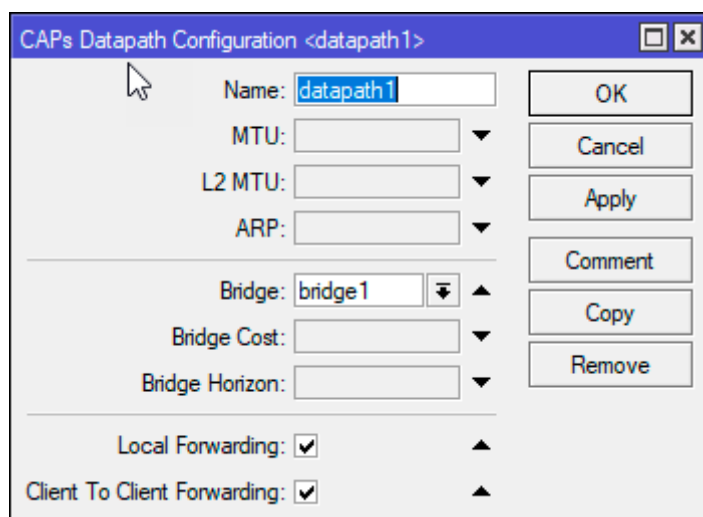
Следующий шаг - настройка шаблонов пересылки данных, для этого перейдем в **CAPsMAN - DataPaths**. Создадим новую настройку и обязательно укажем: **Bridge** - интерфейс сетевого моста, куда будет подключен беспроводной интерфейс после

его активации. Обратите внимание, что выбранное значение применяется ко всем устройствам. В нашем случае bridge1 должен быть интерфейсом локальной сети для всех настраиваемых устройств.

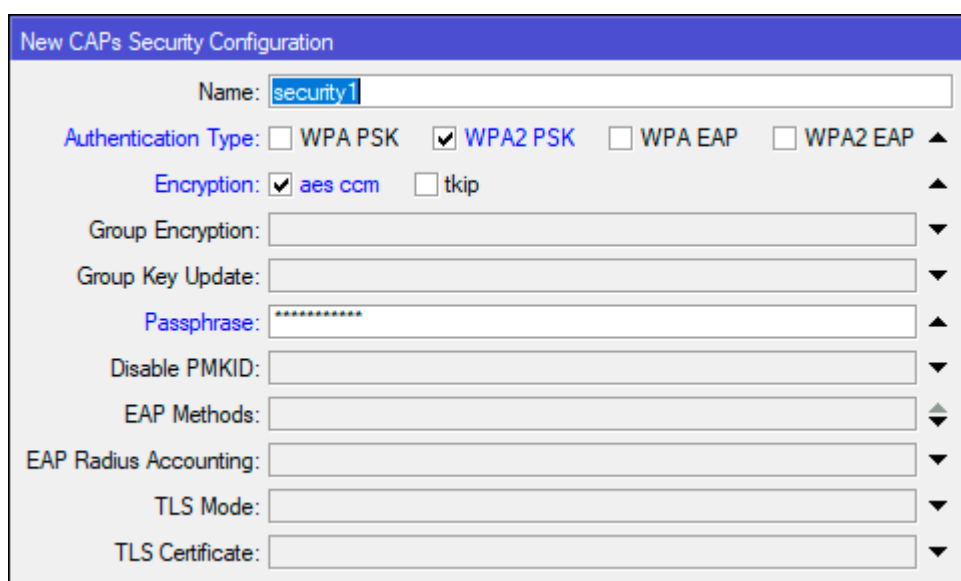
**Local Forwarding** означает, что передачей данных между беспроводными клиентами управляет точка доступа, в противном случае все данные будут пересылаться контроллеру CAPsMAN, а обратно в беспроводную сеть будут отправляться только пришедшие от него данные. Это серьезно увеличивает нагрузку на проводной сегмент сети и должно использоваться только в тех случаях, когда вы действительно собираетесь фильтровать передаваемые данные на контроллере.

**Client To Client Forwarding** включает передачу данных между беспроводными клиентами, в гостевых сетях, в целях повышения безопасности, имеет смысл отключать.

Затем переходим в **CAPsMAN - Security Cfg.** и создаем новую настройку безопасности, здесь все просто, запутаться решительно негде:



The image shows a dialog box titled "CAPs Datapath Configuration <datapath1>". It contains several configuration fields: "Name" (datapath1), "MTU", "L2 MTU", "ARP", "Bridge" (bridge1), "Bridge Cost", "Bridge Horizon", "Local Forwarding" (checked), and "Client To Client Forwarding" (checked). On the right side, there are buttons for "OK", "Cancel", "Apply", "Comment", "Copy", and "Remove".



The image shows a dialog box titled "New CAPs Security Configuration". It contains several configuration fields: "Name" (security1), "Authentication Type" (WPA2 PSK selected), "Encryption" (aes ccm selected), "Group Encryption", "Group Key Update", "Passphrase" (masked with dots), "Disable PMKID", "EAP Methods", "EAP Radius Accounting", "TLS Mode", and "TLS Certificate".

После того, как вы выполнили данные настройки самое время создать конфигурацию, это можно сделать в **CAPsMAN - Configurations**. На вкладке **Wireless** указываем режим работы - **Mode - ap** - точка доступа. Имя беспроводной

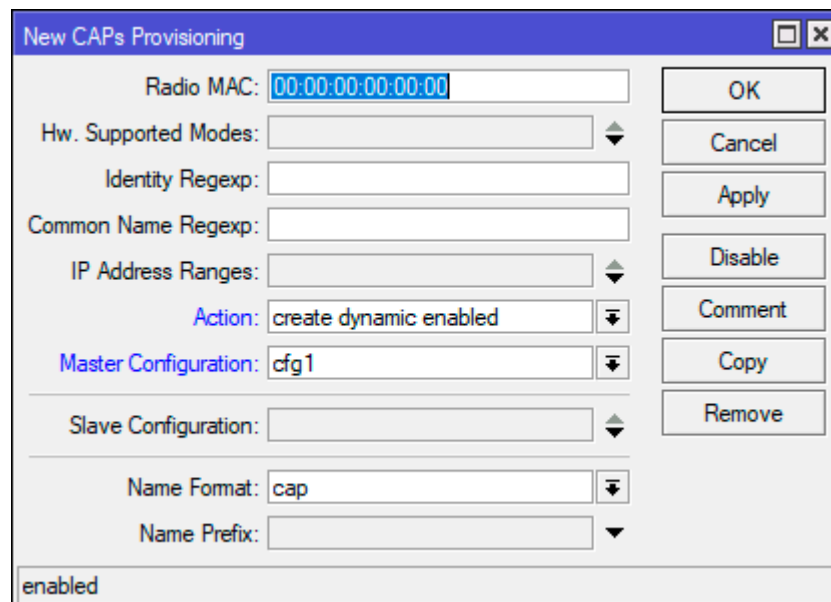
сети - **SSID**, **Country** - страна - **russia3** (для России). Это основные настройки, но также можно указать и дополнительные, скажем **Hw. Protection Mode** - защита от скрытого узла.

The screenshot shows the 'New CAPs Configuration' dialog box with the 'Wireless' tab selected. The 'Name' field is set to 'cfg1'. The 'Mode' is set to 'ap'. The 'SSID' is 'OFFICE'. The 'Country' is 'russia3'. The 'Hw. Protection Mode' is set to 'rts cts'. Other fields like 'Hide SSID', 'Load Balancing Group', 'Distance', 'Hw. Retries', 'Frame Lifetime', 'Disconnect Timeout', and 'Keepalive Frames' are empty. On the right, there are buttons for 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and 'Remove'.

На остальных вкладках указываем уже созданные нами шаблоны, хотя, как альтернатива, можно указать нужные настройки прямо тут.

The screenshot shows the 'New CAPs Configuration' dialog box with the 'Channel' tab selected. The 'Channel' is set to 'channel1'. Other fields like 'Frequency', 'Secondary Frequency', 'Control Channel Width', 'Band', 'Extension Channel', 'Tx Power', 'Save Selected', 'Reselect Interval', and 'Skip DFS Channels' are empty. On the right, there are buttons for 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and 'Remove'.

Созданную нами конфигурацию нужно распространить на точки доступа, за это отвечает настройка разворачивания **CAPsMAN - Provisioning**. Самый простой вариант будет выглядеть так: **Radio MAC** - везде нули, т.е. любая точка доступа, **Action** - **create dynamic enabled** - динамическое создание беспроводного интерфейса на точке доступа, **Master Configuration** - применяемая при создании интерфейса конфигурация.



**New CAPs Provisioning**

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

Hw. Supported Modes: [dropdown]

Identity Regexp: [text box]

Common Name Regexp: [text box]

IP Address Ranges: [dropdown]

Action: create dynamic enabled

Master Configuration: cfg1

Slave Configuration: [dropdown]

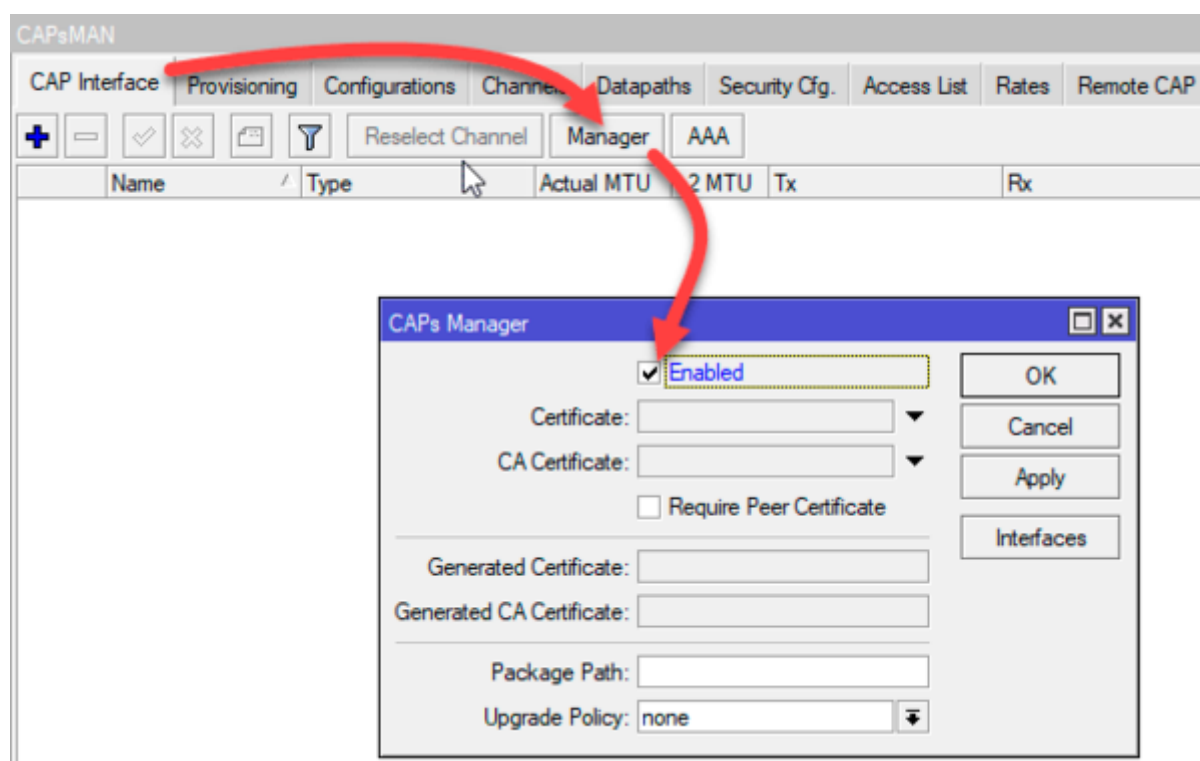
Name Format: cap

Name Prefix: [dropdown]

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

enabled

На этом базовая настройка контроллера завершена, осталось только его включить, для этого в **CAPsMAN - CAP Interface** нажмите кнопку **Manager** и в открывшемся окне установите флаг **Enabled**.



**CAPsMAN**

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

Buttons: +, -, [check], [x], [icon], Reselect Channel, Manager, AAA

Name	Type	Actual MTU	2 MTU	Tx	Rx

**CAPs Manager**

☒ Enabled

Certificate: [dropdown]

CA Certificate: [dropdown]

☐ Require Peer Certificate

Generated Certificate: [text box]

Generated CA Certificate: [text box]

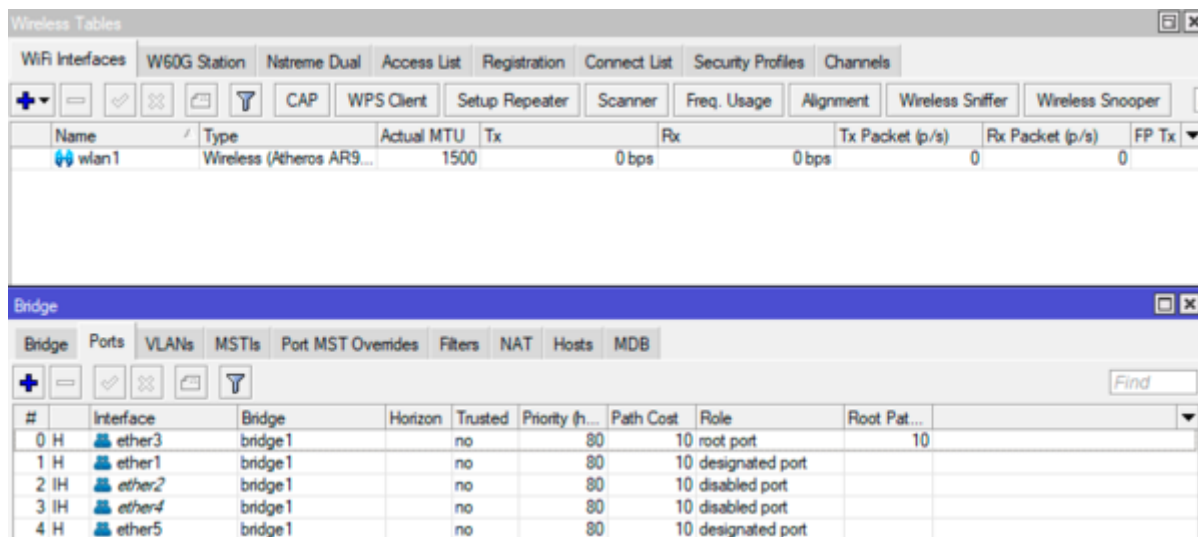
Package Path: [text box]

Upgrade Policy: none

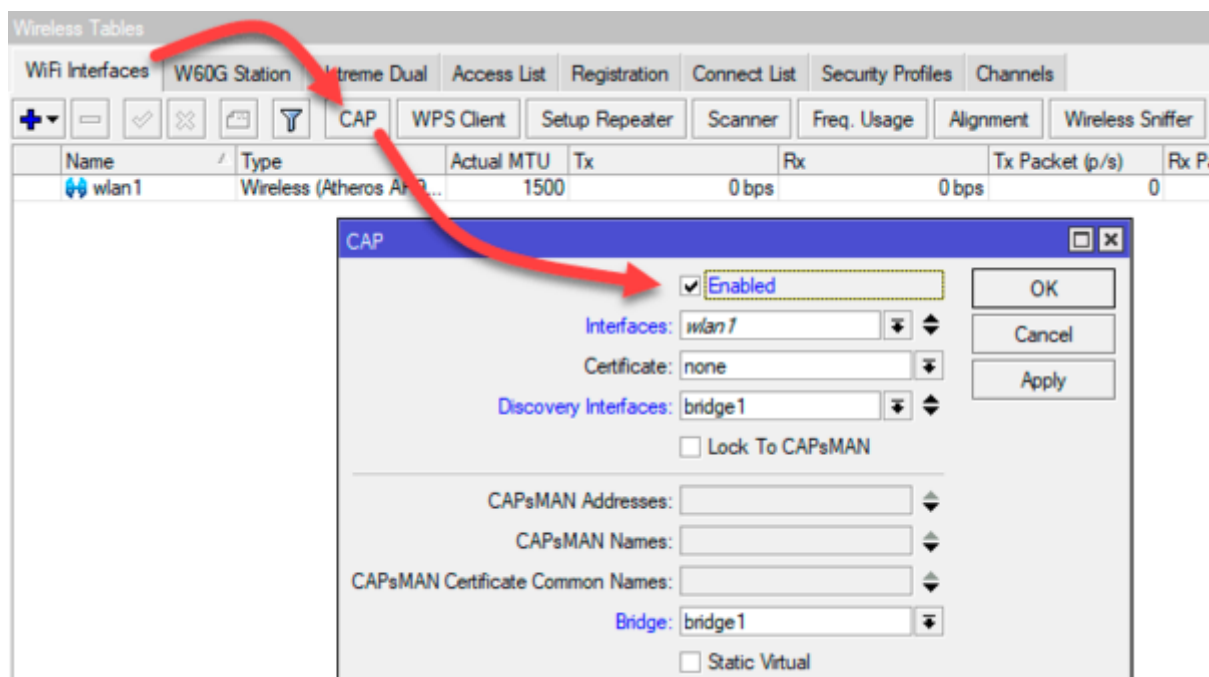
Buttons: OK, Cancel, Apply, Interfaces

Теперь перейдем к настройке точек доступа. Прежде всего убедимся, что беспроводной интерфейс не входит ни в один мост, а мост, смотрящий в локальную сеть, имеет имя **bridge1**, которое мы указали в настройках **Datapath** контроллера.





В **Wireless - WiFi Interfaces** нажимаем кнопку **CAP** и в открывшемся окне устанавливаем флаг **Enabled**, а также указываем: **Interfaces** - беспроводные интерфейсы, которые управляются CAPsMAN, если их несколько - добавляем все, **Discovery Interfaces** - сетевой интерфейс, через который осуществляется связь с контроллером, в нашем случае это тот же мост bridge1, но в более сложных сетях точка может работать в одной сети, а управляться через другую, поэтому стоит разделять эти понятия. **Bridge** - сетевой мост, куда будет подключен беспроводной интерфейс после активации.



После активации данного режима точка обнаружит контроллер и получит от него настройки, созданный интерфейс автоматически присоединится к указанному мосту, подключив беспроводную часть сети к проводной. Аналогичную настройку нужно выполнить на всех остальных точках доступа.



Wireless Tables

WiFi Interfaces

W60G Station

Nstreme Dual

Access List

Registration

Connect List

Security Profiles

Channels

+

−

✓

✕

📄

🔍

CAP

WPS Client

Setup Repeater

Scanner

Freq. Usage

Alignment

Wireless Sniffer

Wireless Snooper

Name

Type

Actual MTU

Tx

Rx

Tx Packet (p/s)

Rx Packet (p/s)

FP Tx

— managed by CAPsMAN

— channel: 2412/20-Ce/gn(17dBm), SSID: OFFICE, local forwarding

RS

🔗 wlan1

Wireless (Atheros AR9...

1500

12.8 kbps

0 bps

13

0

Bridge

Bridge

Ports

VLANs

MSTIs

Port MST Overrides

Filters

NAT

Hosts

MDB

+

−

✓

✕

📄

🔍

Find

#

Interface

Bridge

Horizon

Trusted

Priority (h...

Path Cost

Role

Root Pat...

0 H

🔗 ether3

bridge1

no

80

10

root port

10

1 H

🔗 ether1

bridge1

no

80

10

designated port

2 IH

🔗 ether2

bridge1

no

80

10

disabled port

3 IH

🔗 ether4

bridge1

no

80

10

disabled port

4 H

🔗 ether5

bridge1

no

80

10

designated port

5 D

🔗 wlan1

bridge1

no

80

10

designated port

Вернемся на контроллер, управляемые точки доступа можно увидеть в **CAPsMAN - CAP Interface**, а подключенных клиентов в **CAPsMAN - Registration Table**, при этом будет указана точка доступа, к которой подключен клиент.

CAPsMAN										
CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table										
CAPs Scanner										
Interface	SSID	MAC Address	EAP Identity	Tx Rate	Rx Rate	Tx Signal	Rx Signal	Uptime	Tx/Rx Pack	
cap1	OFFICE	04:92:26:7C:D1:15		18Mbps	72.2Mbps...	0	-45	00:00:20...	106/101	

Теперь можете отправить кого-нибудь с клиентским устройством походить между точками доступа и посмотрите, как контроллер производит переключение.

Хорошо, когда все точки одинаковые и к ним можно применить одинаковые настройки, но что делать, если это не так и разные точки должны получать разные конфигурации? Нет проблем, прежде всего создадим необходимые конфигурации, а затем выясним MAC-адреса беспроводных интерфейсов точек, это можно сделать на вкладке **CAPsMAN - Radio**. Обратите внимание, что нам нужен именно **Radio MAC**.

CAPsMAN				
CAP Interface Provisioning Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio				
Provision				
Radio MAC	Remote CAP Name	Remote CAP Iden...	Interface	
P C4:AD:34:16:05:90	[C4:AD:34:16:05:...	AP-2	cap3	
P C4:AD:34:61:62:77	[C4:AD:34:61:62:...	AP-1	cap1	

Теперь возвращаемся на вкладку **CAPsMAN - Provisioning** и создаем настройки развертывания для каждой точки, указав ее **Radio MAC**, при этом настройку с нулевым MAC-адресом следует **выключить**, в противном случае к устройству применится именно она, а не персональные настройки.

CAPs Provisioning <C4:AD:34:61:62:72>

Radio MAC: C4:AD:34:61:62:72

Hw. Supported Modes: [dropdown]

Identity Regexp: [text box]

Common Name Regexp: [text box]

IP Address Ranges: [dropdown]

Action: create dynamic enabled [dropdown]

Master Configuration: cfg1 [dropdown]

Slave Configuration: [dropdown]

Name Format: cap [dropdown]

Name Prefix: [dropdown]

enabled

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

На что еще стоит обратить внимание? На скриншоте выше есть две опции: **Name Format** и **Name Prefix**, они отвечают за формат имени беспроводных интерфейсов в **CAPsMAN**, по умолчанию это **capN**, что не слишком информативно, а также по мере изменения настроек номера интерфейсов могут меняться, что добавляет путаницы. Поэтому имеет смысл изменить порядок именования, если мы выберем **identity**, то имена интерфейсов будут формироваться согласно указанному в **System - Identity** имени устройства.

Interface List									
Interface									
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> <div>Detect Internet</div> </div>									
Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)		
DM AP-1-1	CAP Interface	1500	1600	0 bps	0 bps	0	0		
DM AP-2-1	CAP Interface	1500	1600	0 bps	0 bps	0	0		
R bridge1	Bridge	1500	1596	336 bps	24.2 kbps	1	32		
S ether1	Ethernet	1500	1596	0 bps	0 bps	0	0		
RS ether2	Ethernet	1500	1596	73.1 kbps	29.2 kbps	9	1		
S ether3	Ethernet	1500	1596	0 bps	0 bps	0	0		
S ether4	Ethernet	1500	1596	0 bps	0 bps	0	0		
S ether5	Ethernet	1500	1596	0 bps	0 bps	0	0		

CAPsMAN									
CAP Interface									
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> <div>Provision</div> <div>Upgrade</div> <div>Set Identity</div> </div>									
Address	Name	Board	Serial	Version	Identity	Base MAC	State	Radios	
C4:AD:34:16:05:8B	[C4:AD:34:16...	RB951Ui-2nD	B88C0B6A7B...	6.47.4	AP-2	C4:AD:34:16:05:8B	Run	1	
C4:AD:34:61:62:72	[C4:AD:34:61...	RB951Ui-2nD	B88C0B6EBC5...	6.47.4	AP-1	C4:AD:34:61:62:72	Run	1	

Если точки доступа двухдиапазонные, то можно выбрать в качестве формата имени **prefix identity** и указать префикс подключения, скажем, частотный диапазон, после чего имя интерфейса будет содержать не только наименование устройства, но еще и префикс, что позволит сразу идентифицировать устройство и беспроводной интерфейс в интерфейсе управления контроллера.

Interface List

Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding	LTE
						Detect Internet			
	Name	Type	Actual MTU	L2 MTU	Tx	Rx			
DM	2.4G-AP-1-1	CAP Interface	1500	1600	0 bps	0 bps			
DM	2.4G-AP-2-1	CAP Interface	1500	1600	0 bps	0 bps			
R	bridge1	Bridge	1500	1596	0 bps	10.1 kbps			
S	ether1	Ethernet	1500	1596	0 bps	0 bps			
RS	ether2	Ethernet	1500	1596	69.8 kbps	12.1 kbps			
S	ether3	Ethernet	1500	1596	0 bps	0 bps			
S	ether4	Ethernet	1500	1596	0 bps	0 bps			
S	ether5	Ethernet	1500	1596	0 bps	0 bps			

В данном материале мы рассмотрели далеко не все возможности CAPsMAN, ограничившись базовыми настройками для быстрого старта, более глубокая настройка требует более широких знаний и будет являться предметом отдельных статей.

### Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на [углубленном курсе по администрированию MikroTik](#). Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.

Помогла статья? Поддержи автора и новые статьи будут выходить чаще:



Или подпишись на наш Телеграм-канал:

- **Категории:**
  - [MikroTik](#),
  - [Сети и интернет](#),
  - [Системному администратору](#).
- **Теги:**
  - [CAPsMAN](#),
  - [MikroTik](#),
  - [Wi-Fi](#),
  - [Сетевые технологии](#)