





#### **MBUM #5**

#### Warszawa 2021





#### **Ihor Hreskiv** MikroTik Certified Trainer

Jestem miłośnikiem urządzeń MikroTik-a od kilku lat

Potrafię wyjść z VIM : )

Korzystam z systemów wirtualizacji dla testowania oraz wdrożenia

Najczęściej używam CHR





# PIERWSZE KROKI

## Planowanie





#### Planowanie Ekahau Pro

ccess Points Surve	eys Building		Signal Strength 👻
earch		36	
owing:4/4 APs	Quick Select Acti	ons 🔻	
retail-store (4/4 AF	s), 8 radios selected		Planning Survey
* 2=3-4-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-	My MiktoTik cAP AC 1		retail-store V +
	<b>6</b> 3.5 m		
retail-store	(n44) 3.5 m 🔥 🕗 🛓 📕 Edit	l	
•	My MiktoTik cAP AC 2		
	6 3.5 m 🕞 Edit	I	
、長い当社時に当 retail-store	📕 📊 44) 3.5 m 🕙 🛃 🚺 Edit	I	
•	My MiktoTik cAP AC 3	B	
	📶 3.5 m 💽 💽 📕 Edit	12-00	1 Jan
	(n36) 3.5 m (), Edit		<ul> <li>• • • • • • • • • • • • • • • • • • •</li></ul>
retail-store	My MiktoTik cAP AC 4		
हिंग दिन्द्र	3.5 m 🔿 🚺 📕 Edit	]	
	$\bigcirc$ $35 \text{ m}$ $\bigcirc$ $\bigcirc$ $\bigcirc$ Edit	1	
retail-store		1	
			PRELIMINARY FLOOR





#### Planowanie NetSpot

City Public Internet Access	dB	Zone surveys: #1 Nov 26, 2016 -
06:27:22:AD:64:49/06		-4
C2:9F:DB:9D:73:44 / C2	-	
🗌 🔴 C2:9F:DB:9D:75:53 / C2	-	
Guest AP	dB	
🗌 📵 0A:18:D6:5B:AC:9E / 0A	-	
OA:18:D6:5B:B0:94 / OA	-	
✓ STAFF	dB	3.94 1.
9 F4:CF:E2:B2:30:FB / Cis	-	
69 F4:CF:E2:C3:B4:BB / Cis	-	
e F4:CF:E2:DB:06:BB / Cis	-	
6 F4:CF:E2:E3:21:7B / Cis	-	
🗍 😑 F4:CF:E2:E3:22:9B / Cis	-	
69 F4:CF:E2:E7:4C:2B / Cis	-	
(a) F4:CF:E2:ED:38:BB / Cis	-	
STAFF LOW	dB	
F4:CF:E2:B2:30:F5 / Cis	- 21,10	
F4:CF:E2:C3:B4:B5 / Cis	-	
F4:CF:E2:DB:06:B5 / Cis		
69 F4:CF:E2:E3:21:75 / Cisc	-	
<b>F4:CF:E2:E3:22:95 / Cis</b>	-	
69 F4:CF:E2:E7:4C:25 / Cis	-	6.3
69 F4:CF:E2:ED:38:B5 / Cis	-	<u>Ø1.2m</u>
TENET-Wi-Fi	dB	
00:27:22:AD:64:49 / Ub	-	
DC:9F:DB:9D:72:B0 / Ub	-	
DC:9F:DB:9D:73:44 / Ub	-	
DC:9F:DB:9D:75:53 / Ub	-	
🗸 🗖 Terminal 42 Guests	dB	
F4:CF:E2:B2:30:F3 / Cis	-	
F4:CF:E2:B2:30:FC / Cis	-	
• F4:CF:E2:C3:B4:B3 / Cis	-	
F4:CF:E2:C3:B4:BC / Cis	33.024	
F4:CF:E2:DB:06:B3 / Cis	-	
F4:CF:E2:DB:06:BC / Cis	-	
• F4:CF:E2:E3:21:73 / Cisc	-	
• F4:CF:E2:E3:21:7C / Cis		
• F4:CF:E2:E3:22:93 / Cis	-	
• F4:CF:E2:E3:22:9C / Cis	-	





#### **Planowanie** WiFi Explorer Pro (MacOS)

		Active			Scanning: Wi-Fi	i   crew		_ □	36 80 MHz	MCS 8	NSS 2 780 Mbps	≋⊚ ∻				α
> Network Name	20	🛅 Default	≎ 🖓 All	2.4 GHz 5 GHz	Open Secure									Q	Y Filter	
✓ Mode	4	BSSID	Network Na ^	Vendor	Annotations	Sig	gnal	Channel	Chann	el Width	Band	Country Co	de Mode	Generation	Security	Max
802.11b/g		E8:94:FC:0D:7C	Renters.pl	P TP-Link T		() 8-	5 dBm 🚺		6	40 MHz	2.4 GHz	PL	b/g/n	Wi-Fi 4	WPA/WPA2 (PSK)	
802.11b/g/n		E4:C3:2A:01:EE	bama12 🔒	P TP-Link T		Ø -8	2 dBm 🔳		3	40 MHz	2.4 GHz		b/g/n	Wi-Fi 4	WPA2 (PSK)	
302.11g/n		C4:AD:08:E2:35	crew 🔒	🔘 MikroTik		<b>Ø</b> -7	7 dBm 📃 📄		36	80 MHz	5 GHz		a/n/ac	Wi-Fi 5	WPA2 (PSK)	
> Channel	15	74:4D:4:D6:F9	crew	🔘 MikroTik		Ø -5	7 dBm 📃		36	80 MHz	5 GHz		a/n/ac	Wi-Fi 5	WPA2 (PSK)	
> Channel Width	3	74:4D:24:D6:F8	crew 🔒	🕓 MikroTik		Ø -5	2 dBm 📃		11	20 MHz	2.4 GHz		g/n	Wi-Fi 4	WPA2 (PSK)	
Security	4	C4:AD:6E:49:27	crew 🔒	🕓 MikroTik		<b>Ø</b> -4	8 dBm 📃		36	80 MHz	5 GHz		a/n/ac	Wi-Fi 5	WPA2 (PSK)	
Access Point	23	C4:AD:6E:49:26	crew 🔒	🕓 MikroTik		Ø -4	2 dBm 📃		1	20 MHz	2.4 GHz		g/n	Wi-Fi 4	WPA2 (PSK)	
✓ Vendor	11	12:A0:9F7:F2:0E	DIRERAVIA	Mitsumi El		Ø -8	3 dBm 📒 🗌		5	20 MHz	2.4 GHz		g/n	Wi-Fi 4	WPA2 (PSK)	
🔯 Cisco Meraki		E8:94:FF:0F:5A	dobr2_end 🔒	₽ TP-Link T		Ø -8	4 dBm 📃		11	20 MHz	2.4 GHz	PL	b/g		WPA/WPA2 (PSK)	
👋 Huawei Technologies		00:BE:37:8F:96	HUA8F96 🔒	🎂 Huawei Te		Ø -7	2 dBm 📃		4	40 MHz	2.4 GHz		<b>b/g/</b> n	Wi-Fi 4	WPA2 (PSK)	
😼 MikroTik		76:4D:2D:FC:45	itechcowo 🔒	🕓 MikroTik		(ý -9	1 dBm 🚺		36	80 MHz	5 GHz		a/n/ac	Wi-Fi 5	WPA2 (PSK)	
Mitsumi Electric		C6:AD:08:E2:35	itechcowo 🔒	🕓 MikroTik		Ø -7	6 dBm 📃		36	80 MHz	5 GHz		a/n/ac	Wi-Fi 5	WPA2 (PSK)	
Netcore Technology Inc.		76:4D:24:D6:F9	itechcowo 🔒	🕓 MikroTik		Ø -5	7 dBm 📃		36	80 MHz	5 GHz		a/n/ac	Wi-Fi 5	WPA2 (PSK)	
N Neigear Inc.		76:4D:24:D6:F8	itechcowo 🔒	🖳 MikroTik		⊘ -5	2 dBm 😑		11	20 MHz	2.4 GHz		g/n	Wi-Fi 4	WPA2 (PSK)	
Philips TP-Link Technologies		C6:AD:6E:49:27	itechcowo 🔒	🔘 MikroTik		⊘ -4	8 dBm 📃		36	80 MHz	5 GHz		a/n/ac	Wi-Fi 5	WPA2 (PSK)	
Unknown Vendor		C6:AD:6E:49:26	itechcowo 🔒	🔘 MikroTik		() -4	2 dBm 🦲		1	20 MHz	2.4 GHz		g/n	Wi-Fi 4	WPA2 (PSK)	
V VTech Telecommunications	5	4A:8F:5B:09:3D	itechcowo 🔒	🕓 MikroTik		Ø -3	4 dBm 🦲		1	20 MHz	2.4 GHz		b <b>/g/</b> n	Wi-Fi 4	WPA2 (PSK)	
ZTE Corp.		E2:CB:A5:DB:40	мсне 🔒	🔯 Cisco Mer		Ø -9	2 dBm		136	40 MHz	5 GHz	PL	a/n/ac	Wi-Fi 5	WPA2 (PSK)	
		E2:CB:AF:0F:3E	мсне 🔒	🔯 Cisco Mer		Ø -9	1 dBm 🚺		112	80 MHz	5 GHz	PL	a/n/ac	Wi-Fi 5	WPA2 (PSK)	
		E0:CB:BF:0F:69	мсне 🔒	🔯 Cisco Mer		Ø -8	7 dBm 🚺 🦳 🗌		6	20 MHz	2.4 GHz	PL	b/g/n	Wi-Fi 4	WPA2 (PSK)	
		EA:CB:AF:0F:3E	MCHE-DZ	Cisco Mer		() -9	1 dBm (		112	80 MHz	5 GHz	PL	a/n/ac	Wi-Fi 5	WPA2 (802.1X)	
						-	Network	Details Signal	Strength	Spectrum A	Advanced Details					
				IS	M				UNII-1	UNII-24	A.			JNII-2C	UNII-3	
		-10														
		-20 itechclour	d cowo													
		an itedficted	B/631vo													20
		-30 C4AD346	BE4926 TP-Link	9A6F	itechck	and co	owo	ju ju	echclaned/	cowq						-30
		-40	Wireless N Router		744D2	28B4D6	F8		crew							4(
		-50			)				744D28B4I	D6F9						-50
		-60	HU	AWEL-8525-85	NET		T-5E5650	ite	e krew	ccwo						-6
		-70	DIRÉCT	-DA-BRAVINCh	ita mileorynaje	Migume	ELGEAR06		03408	-26 <mark>5</mark>						-7
			BRAVA	KDL-40EX650 MOFIE5A:9	Wireless Rou	uterthe	WH 74 Vineless A	P) ite	loud	ow <mark>oo</mark>				MOUE TO		-80
		00							285 DF	-C.4.5			MMBHERDZC	MANDEDEC		01
		-90														
		1	2 3 4	5 6 7	8 9 10	11 1	2 13	14	36 40 44	48 52 56 60	0 64		100 108 116	124 132 140	149 157 165	
								Se MikroTik:B	4:D6:F9, 0	Ch. 36 @ 80	0 MHz					
utomatic Filters 🗸		Networks Found: 38, D	isplayed: 38 (100%)													

7



# HARDWARE / SOFTWARE

## Połączenie do sieci testowej

- Dostęp do Wi-Fi: SSID: mbum#5
- Login: vip
- Hasło: 1234 VLAN: 55
- Login: guest Hasło: 1234 *VLAN:* 77

#### Access points Indoor / Outdoor / Combined







wAP





cAPAC

cAP XL ac



#### Access points cAP XL ac







#### Wi-Fi klienci Wsparcie po stronie klienta / Capabilities

Device	SS	.11	MU-MIMO	.11v	Link
Blackberry Key One	1	ac	Y	Ν	PCAP
Blackberry Passport	1	ac	Ν	Υ	
Dell XPS 15 7590	2	ax	Ν	Υ	PCAP
Google Pixel 4	2	ac	Ν		PCAP
iPhone 11	2	ac	Ν	Υ	PCAP
iPhone 11 Pro	2	ax	Ν	Y	PCAP
iPhone 11 Pro Max	2	ax	N	Y	PCAP
iPhone 12 Pro	2	ax	N	Y	PCAP
Lenovo X1 Carbon	2	ac	N	Y	PCAP
Macbook Pro 2019 16"	3	ac	N	Ν	PCAP
Samsung Galaxy S10	2	ax	Y	Y	PCAP
Samsung Galaxy S10e	2	ax	Y	Y	PCAP
Samsung Galaxy S10+	2	ax	Y	Y	PCAP
Tesla Model S	2	ac	Ν	Y	PCAP

https://clients.mikealbano.com/



## Serwer Radius





Ihor Hreskiv - MikroTik Certified Trainer





#### Server Radius MikroTik User Manager (v7)

User Man	lager							
Sessions	Routers Users User	Groups Profiles User Profiles	Limitations Profile Lim	nitations Attributes Payment				
Clo	se Session Settings	Generate Report						Find
User	🛆 Acct Session I	ID NAS IP Address Calling Statio	n ID User Address	Started	Ended	Terminate Ca	Uptime	•
Inor	84000001	1/2.16.254.3 10.10.1.10		Sep/23/2021 08:48:24	4 Sep/23/2021 08:52:30	User Request	00:04:05	•
ihor	84000001	172.16.254.3 10.10.1.19		Sep/24/2021 07:08:45	5 Sep/24/2021 07:09:04	User Request	00:00:19	
ihor	84000001	172.16.254.2 10.10.1.10		Sep/29/2021 06:39:22	2 Sep/29/2021 06:49:10	) User Request	00:09:47	
oskar	00000086	192.168.10.245 F8-75-A4-6A-	80-13	Aug/11/2021 08:58:28	Aug/11/2021 09:00:11	User Request	00:01:43	
oskar	01000086	192.168.10.245 F8-75-A4-6A-	80-13	Aug/11/2021 09:00:18	Aug/11/2021 11:36:50	Um Nas Rebo		
piotr	05000086	192.168.10.240 00-E0-4C-34-	74-AD	Aug/11/2021 08:58:23	Aug/11/2021 08:59:41	User Request	00:01:18	
piotr	04000086	192.168.10.240 74-4D-28-84-	-4C-EB	Aug/11/2021 08:57:1:	1 Aug/11/2021 09:00:08	3 User Request	00:02:57	
piotr	06000086	192.168.10.240 00-E0-4C-34-	74-AD	Aug/11/2021 08:59:47	7 Aug/11/2021 09:01:25	5 User Request	00:01:37	
piotr	07000086	192.168.10.240 74-4D-28-84-	-4C-EB	Aug/11/2021 09:00:14	4 Aug/11/2021 09:04:18	3 User Request	00:04:04	
piotr	09000086	192.168.10.240 00-E0-4C-34-	74-AD	Aug/11/2021 09:06:00	Aug/11/2021 09:06:58	3 User Request	00:00:58	
piotr	08000086	192.168.10.240 74-4D-28-84-	-4C-EB	Aug/11/2021 09:04:2:	1 Aug/11/2021 09:08:44	User Request	00:04:23	
test	84000003	192.168.10.253 94:05:BB:11:	EF:D7	Aug/11/2021 07:55:40	O Aug/11/2021 07:56:39	User Request	00:00:59	
test	84000003	192.168.10.240 94:05:BB:11:	EF:D7	Aug/11/2021 08:41:27	7 Aug/11/2021 08:41:46	5 Um Nas Rebo		
A tomasz	z 8400004	10.10.1.14 94:05:BB:11:	EF:D7	Sep/15/2021 09:25:03	1			
user-1	0 0300086	192.168.10.253 2C-C8-1B-47-	-03-0D	Aug/11/2021 08:20:07	7 Aug/11/2021 08:22:05	5 User Request	00:01:58	+
171 item	s	···· ··· ··· ··· ··· ···		• • • • • • • • • •			1-	



#### Kontroler MikroTik CAPsMAN

# przetwarzanie danych.

konfiguracja do komunikacji z kontrolerem CAPsMAN.

uwierzytelnianie klienta) są teraz wykonywane przez CAPsMAN.

**Controlled Access Point system Manager (CAPsMAN)** pozwala na centralizowane zarządzanie siecią bezprzewodową i, w razie potrzeby,

- Jeśli CAP jest kontrolowany przez CAPsMAN, wymagana tylko minimalna
- Funkcje, które były zwykle wykonywane przez CAP (np. kontrola dostępu,





# CAP powinien pracować na RouterOS z licencją L4 lub wyższą Nie limitowana ilość CAP-ów, kontrolowanych CAPsMAN-em 32 moduly radiowe na 1 CAP (access point) 32 wirtualne interfejsy radiowe na jednym master interfejsie

#### Kontroler MikroTik CAPsMAN

- CAPsMAN może być uruchomiony na dowolnym RouterBoard oraz CHR



#### Kontroler MikroTik CAPsMAN

CAPsMAN								
CAP Interf	ace Provisioning	Configurations	Channels	Datapaths	Security Cfg.	Access List	Rates	Remote CAP
		Reselect Chanr	nel Mana	ager AAA				
	Name	1	Туре		Actual MTU	J L2 MTU	Tx	
DSMB	🚸 2GHz-AP-conf	-1	CAP Inter	rface	19	500 1600	)	C
DSB	🚸 2GHz-AP-c	onf-1-1	CAP Inter	rface	19	500 1600	)	C
DRSMB	🚸 2GHz-WAP-AG	C-LTE6-1	CAP Inter	rface	19	500 1600	)	C
DSB	🚸 2GHz-WAF	P-AC-LTE6-1-1	CAP Inter	face	1!	500 1600	)	C
DSMB	♦ 2GHz-cAP-AC-	-01-OSP-1	CAP Inter	face	1!	500 1600	)	C
DSB	🚸 2GHz-cAP-	AC-01-OSP-1-1	CAP Inter	rface	1!	500 1600	)	C
DRSMB	↔ 2GHz-cAP-AC-	-office-1	CAP Inter	rface	15	500 1600	)	C
DSB	♦ 2GHz-cAP-	AC-office-1-1	CAP Inter	face	1!	500 1600	)	C
DSMB	↔ 2GHz-cowo-1	50 - M3	CAP Inter	rface	19	500 1600	)	C
DSB	♦ 2GHz-cow	o-1-1	CAP Inter	rface	15	500 1600	)	C
DSMB	♦ 5GHz-AP-conf	-1	CAP Inter	rface	1	500 1600	)	0
DSB	↔ 5GHz-AP-c	onf-1-1	CAP Inter	rface	1	500 1600	)	0
DSMB	♦ 5GHz-WAP-AC	C-LTE6-1	CAP Inter	rface	1!	500 1600	)	C
DSB	🚸 5GHz-WAF	P-AC-LTE6-1-1	CAP Inter	rface	1	500 1600	)	C
DSMB	♦ 5GHz-cAP-AC-	-01-OSP-1	CAP Inter	rface	15	500 1600	)	C
•			leas s		ti tes		du .	
20 items ou	ut of 40							R.

Radio Registration Table

Tx Packet (p/s) FP Tx Pacl 🔻 Rx Packet (p/s) FP Tx FP Rx Rx 0 bps 0 bps 0 bps bps 0 0 0 bps bps 0 bps 0 0 bps 0 bps 0 bps 0 0 bps 0 bps 0 bps 0 bps 0 bps 0 bps 0 0 bps 0 bps 0 0 0 bps 0 bps bps 0 bps 0 bps 0 bps 0 0 bps 0 bps 0 0 bps 0 bps 0 bps 0 bps 0 bps 0 bps 0 0 bps 0 bps 0 0 0 bps 0 bps bps 0 0 bps 0 0 bps 0 bps bps 0 bps 0 0 bps 0 bps 0 bps 0 bps 0 bps 0 bps 0 0 bps 0 bps 0 0 0 bps 0 bps bps 0 bps 0 0 bps 0 bps 0 bps 0 bps 0 0 bps 0 bps 0



# SCHEMAT / KONFIGURACJA

## Schemat sieci





Ihor Hreskiv - MikroTik Certified Trainer



# Konfiguracja Certyfikat Let's Encrypt

Certificate <letsencrypt-autogen_2021-09-29t06:58:33z></letsencrypt-autogen_2021-09-29t06:58:33z>		
General Key Usage Status	ОК	
Name: letsencrypt-autogen_2021-09-29T06:58:33Z	Cancel	
Issuer: C=US,O=Let's Encrypt,CN=R3	Apply	
	Сору	Dostepny w ROSv7
	Remove	
Country:	Sign	
State:	Sign via SCEP	
Locality:	Create Cert. Request	Certificate <letsencrypt-autogen 2021-09-29t06.58.337=""></letsencrypt-autogen>
Organization:	Import	Control Koy Llongo Chatta
Unit:	Card Reinstall	General Rey Usage Status
Common Name: mbum.mtik.pl	Card Verify	Key Usage: digital signature
Subject Alt. Name: DNS : mbum.mtik.pl	Export	key encipherment
Key Type: RSA	Revoke	tls client
Key Size: 2048		tls server
Days Valid: 89		
✓ Trusted		
private key crl authority revoked expired smart card key trust	ed	

#### /certificate/enable-ssl-certificate dns-name=mbum.mtik.pl



### Konfiguracja Radius serwer / User Manager (v7)

User Manager					
Sessions Routers Users User Groups Profiles User Profiles Lin	mitations Profile Limit	ations Attributes P	ayment		
Close Session Settings Generate Report					Find
User 🛆 Acct Session ID NAS IP Address Calling Station I	D User Address	Started	Ended	Terminate Ca	Uptime 🔻
	Settinas				
0 items		Fnabled			OK
	Authentication Port:	1812			Cancel
	Addientication Fort.	1012			
	Accounting Port:	1813			Арріу
	Certificate:	letsencrypt-autogen	_2021-09-29T06:58:332	Z 두 🔺	Database
		Use Profiles			Advanced
	Active Sessions:	0			



#### Konfiguracja Radius serwer / User Manager (v7)

Router <local-chr></local-chr>			
Name:	local-chr	ОК	
Shared Secret:	*****	Cancel	
Address:	127.0.0.1	Apply	
CoA Port:	3799	Disable	
Access Requests:	104	Сору	
Access Failures:	10	Remove	
Broken Requests:	0	Reset Counters	
Unknown Requests:	0		
Accounting Requests:	23		
Accounting Failures:	22		
Disconnect Ack:	0		
Disconnect Nak:	0		
CoA Ack:	0		
CoA Nak:	0		
Sent From Cache:	31		
enabled			

W danej demonstracji wykorzystano połączenie do *localhost* 

W środowisku produkcyjnym należy dodać wszystkie CAP-y lub inne urządzenia który będą korzystać z uwierzytelnienia za pomocą serwera Radius



#### Konfiguracja Radius serwer / Użytkownicy

Parametr Mikrotik-Wireless-VLANID podajemy inny dla każdego z użytkowników, dla przypisania do różnych VLAN

Dla demonstracji wykorzystano parametr **Shared Users - 250**, co pozwoli z wykorzystania takiego samego konta do 250 razy Pa OTF

User <

Gener

Ca

At

enable

User <\

Genera

Pa: OTP

Ca Shared

Att

enabled

guest>					
al Statu	s			1	ОК
Name:	guest				Cancel
ssword:	****				Apply
Secret:					Disable
Group:	default			₹	Сору
aller ID:				Ŧ	Remove
d Users:	250				Generate Voucher
tributes:	Mikrotik-Wireless-VLANID	₹ :	77	<b>\$</b>	
	Mikrotik-Wireless-VLANIDtype	₹ :	0	] ♦	
d					

/ip>		
al Statu	S	ОК
Name:	vip	Cancel
ssword:	****	Apply
Secret:		Disable
Group:	default	Сору
aller ID:		Remove
Users:	250	Generate Voucher
ributes:	Mikrotik-Wireless-VLANID	
	Mikrotik-Wireless-VLANIDtype 🗧 : 0	
1		



#### **Uwierzytelnienie** CAPsMAN / Radius

RADIUS Server <127.	0.0.1>	
General Status		ОК
Service:	ppp 🔽 login	Cancel
	hotspot 🗸 wireless	Apply
	dhcp ipsec	Disable
	✓ dot1x	Comment
Called ID:		Сору
Domain:		Remove
Address:	127.0.0.1	Reset Status
Protocol:	udp.	
Secret:	*****	
Authentication Port:	1812	
Accounting Port:	1813	
Timeout:	300 ms	
	Accounting Backup	
Realm:		
Certificate:	none	
Src. Address:	0.0.0	
enabled		

Na kontrolerze CAPsMAN konieczne dodanie korzystania z serwera Radius



# **Uwierzytelnienie** CAPsMAN / Security Cfg. / WPA2-EAP

CAPs Securit	CAPs Security Configuration <sec-eap></sec-eap>							
	Name:	sec-eap						
Authentio	cation Type:	WPA PSK WPA2 PSK WPA EAP WPA2 EAP						
	Encryption:	🖌 aes ccm 📃 tkip		-				
Group	Encryption:	aes ccm	₹					
Group I	Key Update:							
	Passphrase:			•				
Disa	able PMKID:							
E/	AP Methods:	passthrough	₹					
EAP Radius	Accounting:							
	TLS Mode:							
TLS	6 Certificate:							





### Konfiguracja CAPsMAN / Datapath

Local Forwarding "rozkazuje" przetwarzać ruch bezpośrednio na access point-ach

Dla konfiguracji *Datapath* wskazujemy VLAN Mode - use tag, ale nie wskazujemy VLAN ID Ten parametr będzie przydzielony dynamicznie z serwera Radius

CAPs D	atapath Configuration	<data-eap-dynamic></data-eap-dynamic>		
	Name:	data-eap-dynamic		ОК
	MTU:		-	Cancel
	L2 MTU:		-	Apply
	ARP:		•	Comment
	Bridge:		•	Сору
	Bridge Cost:		-	Remove
	Bridge Horizon:		-	
	Local Forwarding:	✓		
Client	To Client Forwarding:		•	
	VLAN Mode:	use tag 두		
	VLAN ID:		-	
	Interface List:		•	



#### Konfiguracja CAP Local forwarding

Wskazanie Bridge jest obowiązkowe na CAP, dla dodania bezprzewodowych interfejsów do lokalnego bridge-a oraz przetwarzania ruchu klientów Wi-Fi na access point a nie CAPsMAN-ie, co zwiększa wydajność całego systemu.





# Konfiguracja CAP Bridge

Bridg	je						
Bric	lge	Ports	Port Extensions	VLANs	MSTIs	Port MST O	verrides
#		Inte	erface	Bridge		Horizon	Trusted
0	D	<b>&amp; I</b>	wlan2	bridge-ca	apsman		no
1	D	<b>#</b> 1	wlan1	bridge-ca	apsman		no
2 ite	ms						

Radiowe interfejsy dodają się jako porty tagowane (trunk)



Ważne jest nie włączenie Bridge VLAN Filtering, inaczej nie będzie możliwości dynamicznego przydziału VLAN-ów dla klientów!!!

https://forum.mikrotik.com/viewtopic.php?f=7&t=176572



#### Uwierzytelnienie WPA2-EAP

CAPsMAN										
CAP Interface	Pro	visioning	Configurations	Channels	Datapaths	Security Cfg.	Access List	Rates F	Remote CAP	Radi
	- T CAPs Scanner									
Interface	Δ	SSID	MAC	Address	EA	P Identity	Tx Rate A	Rx Rate	Tx Signal	Rx
2GHz-cAP-XL-A	C-1	mbum#5	5 9C:E	0:63:92:40	C:4D vip	)	54Mbps 6	55Mbps		0
5GHz-cAP-XL-A	C-1	mbum#5	5 90:9	C:4A:BA:F	1:C7 gu	est	5Mbps 7	780Mbps		0

Klienci na liście Registration Table, poprawnie uwierzytelnione z nazwami użytkowników *vip* oraz *guest*  **?** 

#### mbum#5

IP Address: 192.168.77.253 Router: 192.168.77.1 Security: WPA2 Enterprise BSSID: 2c:c8:1b:ef:63:27 Channel: 36 (5 GHz, 80 MHz) Country Code: PL RSSI: -44 dBm Noise: -92 dBm Tx Rate: 780 Mbps PHY Mode: 802.11ac MCS Index: 9 NSS: 2

#### Klient MAC OS



## Dziękuję za uwagę

#### Materiały oraz konfigurację https://ua.mwtc.pl/mbum5/





Ihor Hreskiv - MikroTik Certified Trainer

#### Kontakt do mnie: e-mail: *ihor@hreskiv.pl*



# MANUAL KROK PO KROKU

Host: mbum.mtik.pl Login: admin Hasło: brak

SSTP użytkownik (dla tunelu): Login: remote-cap Hasło: mbum#5

Dostęp do «żywego» CHR

Dostęp do CHR (Radius+CAPsMAN):

### Konfiguracja user-manager Instalowanie paczki

# Należy pobrać paczkę user-manager dla odpowiedniej architektury ze strony *mikrotik.com/download/*

RouterOS 🔝	
	6.47.10 (Long-term)
MIPSBE	CRS1xx, CRS2xx, CRS312-4C+8XG, CRS32 2, mAP, mAP lite, NetBox, NetMetal, PowerBo RB7xx, hEX PoE
Main package	
Extra packages	
ARM64	nRAY, CCR2004, LHGGR
Main package	
Extra packages	
The Dude server	

6.48.4 (Stable)

6.49rc2 (Testing)

7.1rc4 (Development)

26-24S+2Q+, CRS354, Cube Lite60, DISC, FiberBox, hAP, hAP ac, hAP ac lite, LDF, LHG, LHG Lite60, ItAP mini, mANTBox, mANTBox ox, PWR-Line, QRT, RB9xx, SXTsq, cAP, hEX Lite, RB4xx, wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant,

8	
	-

?

#### Konfiguracja user-manager Instalowanie paczki

Po rozpakowaniu archiwum .zip za pomocą ftp, webfig lub winbox-a przekazać plik user-manager-7.1rc4.npk do folderu korzeniowego (root folder) i zrestartować urządzenie.

> calea-7.1rc4.npk container-7.1rc4.npk gps-7.1rc4.npk iot-7.1rc4.npk

```
tr069-client-7.1rc4.npk
user-manager-7.1rc4.npk
```

#### Konfiguracja user-manager Uruchomienie serwera Radius

#### Po restarcie urządzenia należy uruchomić serwer Radius, podając certyfikat

			ihor@mbum.n	ntik.pl (mbum.mtik	.pl) - WinBox (64bit) v7.1					
Session Settings Dashl	ession Settings Dashboard									
Safe Mode Se	ession: mbum.mtik.pl									
🗡 Quick Set	User Manager	Settings								
	Sessions Routers Users User		✓ Enabled	ОК						
Ser Manager	Close Session Settings	Authentication Port:	1812	Cancel	Find					
Wireless	User 🛆 Acct Session I	Accounting Port:	1813	Apply	Terminate Ca Uptime					
I WireGuard		Certificate:	letsencrypt-autogen_2021-09-29T06:58:33Z	▲ Database						
🔀 Bridge			Use Profiles	Advanced						
PPP		Active Sessions:	0							
Mesh										
₽ IP	•				•					
MPLS	0 items									

## /user-manager set certificate=letsencrypt-aut

set certificate=letsencrypt-autogen\_2021-09-29T06:58:33Z enabled=yes

#### Konfiguracja user-manager Dodawanie router-a

#### Dodajemy router do user-managera

/user-manager/router/add shared-secret=1234 address=127.0.0.1

Router <local-chr> Name: local-chr OK Shared Secret: \*\*\*\*\*\*\* Cancel Address: 127.0.0.1 Apply CoA Port: 3799 Disable Access Requests: 125 Сору Access Failures: 27 Remove Reset Counters Broken Requests: 0 Unknown Requests: 0 Accounting Requests: 1 Accounting Failures: 0 Disconnect Ack: 0 Disconnect Nak: 0 CoA Ack: 0 CoA Nak: 0 Sent From Cache: 54 enabled

# Konfiguracja user-manager Dodawanie użytkownika

User <vip></vip>							
General Statu	ОК						
Name:	Name: vip						
Password:	****			Apply			
OTP Secret:				Disable			
Group:	default		<b>.</b>	Сору			
Caller ID:			<b>T</b>	Remove			
Shared Users:	250			Generate Voucher			
Attributes:	Mikrotik-Wireless-VLANID	₹:55	<b></b>				
	Mikrotik-Wireless-VLANIDtype	▼:0	•				
enabled							

/user-manager user add attributes=Mikrotik-Wireless-VLANID:55,Mikrotik-Wireless-VLANIDtype:0 name=vip shared-users=250



#### Konfiguracja Radius Dodajemy korzystanie z Radius-a

	MIPLS		DADTUS Conver <127	0.0.1			
-6	IPv6		RADIOS SEIVEI <127.	.0.0.1>	-		
S	Routing		General Status			ОК	
<b>O</b>	System 🖹		Service:	ppp 🔽 login		Cancel	
9	Queues			hotspot 🗸 wireless		Apply	
	Files			dhcp ipsec		Disable	
	Log			✓ dot1×		Comment	
	RADIUS	RADIUS				Сору	
	Tools	+	Called ID:			Remove	Find
>	New Terminal	# Servi	Domain:		┍		tificate 🔻
<b>~&gt;</b>	Dot1X	0 login	Address:	127.0.0.1		Reset Status	
	Make Supout.rif		Protocol:	udp 3	Ŧ		
	New WinBox		Secret:	****			
	Exit						
			Authentication Port:	1812			
	Windows	•	Accounting Port:	1813			•
		1 item (1 se	Timeout:	300 m	าร		
				Accounting Backup			
			Realm:		-		
			Certificate:	none	Ŧ		
			Src. Address:	0.0.0.0			
			enabled				

/radius
add address=127.0.0.1 service=]

#### add address=127.0.0.1 service=login,wireless,dot1x secret=1234

### Konfiguracja CAPsMAN Security Cfg.

CAPs Security Configuration <sec-eap></sec-eap>	
Name: sec-eap	ОК
Authentication Type: WPA PSK WPA2 PSK WPA EAP VPA2 EAP	Cancel
Encryption: 🗹 aes ccm 🗌 tkip	Apply
Group Encryption: aes ccm	Comment
Group Key Update:	Сору
Passphrase:	Remove
Disable PMKID:	
EAP Methods: passthrough	•
EAP Radius Accounting: 🗹	
TLS Mode:	
TLS Certificate:	

/caps-man security
add authentication-types=wpa2-eap eap-methods=passthrough eap-radiusaccounting=yes encryption=aes-ccm group-encryption=aes-ccm name=sec-eap

### Konfiguracja CAPsMAN Datapath

CAPs Datapath Configuration	<da< th=""></da<>
Name:	dat
MTU:	
L2 MTU:	
ARP:	
Bridge:	
Bridge Cost:	
Bridge Horizon:	
Local Forwarding:	~
Client To Client Forwarding:	
VLAN Mode:	use
VLAN ID:	
Interface List:	

/caps-man datapath
add local-forwarding=yes name=data-eap-dynamic vlan-mode=use-tag



### Konfiguracja CAPsMAN Channels

CAPs Channel <ch-2></ch-2>			
Name:	ch-2		ОК
Frequency:	2412	\$	Cancel
	2432	\$	Apply
	2452	<b>\$</b>	Comment
Secondary Frequency:		•	Сору
Control Channel Width:	20Mhz		Remove
Band:	2ghz-onlyn		
Extension Channel:	disabled 🔻		
Tx Power:	13	]	
Save Selected:		•	
Reselect Interval:			
Skip DFS Channels:			

#### /caps-man channel

add band=2ghz-onlyn control-channel-width=20mhz extension-channel=disabled frequency=2412,2432,2452 name=ch-2 tx-power=13 add band=5ghz-onlyac control-channel-width=20mhz extension-channel=XXXX name=ch-5 skip-dfs-channels=yes tx-power=20

Name:	ch-5			ОК
Frequency:			\$	Cancel
Secondary Frequency:			\$	Apply
Control Channel Width:	20Mhz	₹		Comment
Band:	5ghz-onlyac	₹		Сору
Extension Channel:	XXXX	₹		Remove
Tx Power:	20		<b></b>	
Save Selected:			-	
Reselect Interval:			-	
Skip DFS Channels:	<ul> <li>Image: A second s</li></ul>		<b></b>	

## Konfiguracja CAPsMAN Configurations

CAPs Configuration <cf< th=""><th>j-vip-2&gt;</th><th></th></cf<>	j-vip-2>	
Wireless Channel Ra	tes Datapath Security	ОК
Name	cfg-vip-2	Cancel
Mode	ap 두 🔺	Apply
SSID	mbum#5	Comment
Hide SSID		Сору
Load Balancing Group		Remove
Distance	indoors 🛛 🐺 km 🔺	
Hw. Retries		
Hw. Protection Mode	rts cts	
Frame Lifetime		
Disconnect Timeout		
Keepalive Frames		
Country	poland 🔻 🔺	
Installation	indoor 두 🔺	
Max Station Count		
Multicast Helper	full 두 🔺	
HT Tx Chains		
HT Rx Chains		
HT Guard Interval		

CAPs Confi	guration <	<cfg-vip< th=""><th>-2&gt;</th><th></th><th></th><th></th></cfg-vip<>	-2>			
Wireless	Channel	Rates	Datapath	Security		ОК
Channel: ch-2						Cancel
	Freque	ncy:				Apply

APs Confi	guration <	<cfg-vip< th=""><th>-2&gt;</th><th></th><th></th><th></th></cfg-vip<>	-2>			
Wireless	Channel	Rates	Datapath	Security		ОК
	Rat	e: rate	s-2	₹		Cancel
Basic Rates						Apply

CAPs Confi	iguration	<cfg-vip< th=""><th>-2&gt;</th><th></th><th></th><th></th></cfg-vip<>	-2>			
Wireless	Channel	Rates	Datapath	Security		ОК
	Datapath: data-eap-dynamic ∓ 🔺					
		MTU			-	Apply

CAPs Confi	guration <	<cfg-vip< th=""><th>-2&gt;</th><th></th><th></th><th></th><th></th></cfg-vip<>	-2>				
Wireless	Channel	Rates	Datapath	Security			ОК
Security: sec-eap 두 🔺						Cancel	
Auther	ntication T	ype:				-	Apply

#### Konfiguracja CAPsMAN Configurations

/caps-man configuration add channel=ch-2 country=poland datapath=data-eap-dynamic distance=indoors hw-protection-mode=rts-cts installation=indoor mode=ap multicast-helper=full name=cfg-vip-2 rates=rates-2 security=sec-eap ssid=mbum#5 add channel=ch-5 country=poland datapath=data-eap-dynamic distance=indoors hw-protection-mode=rts-cts installation=indoor mode=ap multicast-helper=full name=cfg-vip-5 security=sec-eap ssid=mbum#5

### Konfiguracja CAPsMAN Provisioning

CAPs Provisioning <00:00	:00:00:00:00>		
Radio MAC:	00:00:00:00:00		OK
Hw. Supported Modes:	gn 두	\$	Cancel
Identity Regexp:			Apply
Common Name Regexp:			Disable
IP Address Ranges:		\$	Comment
Action:	create dynamic enabled	₹	Сору
Master Configuration:	cfg-vip-2	Ŧ	Remove
Slave Configuration:		\$	
Name Format:	prefix identity	₹	
Name Prefix:	2GHz	<b>A</b>	
enabled			

Radio MAC:	00:00:00:00:00	ОК
Hw. Supported Modes:	ac 두 🖨	Cancel
Identity Regexp:		Apply
Common Name Regexp:		Disable
IP Address Ranges:		Comment
Action:	create dynamic enabled 🗧	Сору
Master Configuration:	cfg-vip-5 ∓	Remove
Slave Configuration:		
Name Format:	prefix identity	
Name Prefix:	5GHz	

#### Konfiguracja CAPsMAN Provisioning

/caps-man provisioning

- add action=create-dynamic-enabled hw-supported-modes=gn \
   master-configuration=cfg-vip-2 name-format=prefix-identity \
   name-prefix=2GHz
- add action=create-dynamic-enabled hw-supported-modes=ac \
   master-configuration=cfg-vip-5 name-format=prefix-identity \
   name-prefix=5GHz

# Konfiguracja CAPsMAN Uruchomienie kontrolera

CAPsMAN	CAPs Manager		
CAP Interface Provisioning Configurations Channels Data	✓ Enabled	ОК	
- C C E Y Reselect Channel Manager	Certificate:	✓ Cancel	
	CA Certificate:	<ul> <li>Apply</li> </ul>	
	Require Peer Certificate	Interfaces	
	Generated Certificate:		
	Generated CA Certificate:	CAPs Manager Inte	erfaces 🗖
	Package Path:		Find
	Upgrade Policy: none	▼ Interface all	△ Forbid
		ether1	yes
/caps-man manager set enabled=yes		2 items	
/caps-man manager inter	face		

add disabled=no forbid=yes interface=ether1



## Konfiguracja CAP Bridge

Interface <bridge-cap< th=""><th>sman&gt;</th><th></th><th></th><th>Interface <bridge-capsman></bridge-capsman></th></bridge-cap<>	sman>			Interface <bridge-capsman></bridge-capsman>
General STP VLAN	Status Traffic		ОК	General STP VLAN Status Traffic
Name	bridge-capsman		Cancel	Protocol Mode:
Туре	: Bridge		Apply	Priority: 8000 hex
MTU	:		Disable	Deciep Nepert
Actual MTU	: 1500		Comment	Perion Povisiont
L2 MTU	1600		Сору	
MAC Address	2C:C8:1B:EF:63:27	7	Remove	
ARP	enabled	₹	Torch	
ARP Timeout	•			Interface <bridge-capsman></bridge-capsman>
Admin. MAC Address				General STP VLAN Status Traffic
Ageing Time	00:05:00			VLAN Filtering
	IGMP Snooping			
	DHCP Snooping			
	✓ Fast Forward			

## /interface bridge add name=bridge-capsman protocol-mode=none vlan-filtering=no

	Konfig	jur W	acja C	AP AP
CAP				
	✓ Enabled		ОК	
Interfaces:	wlan1	₹ \$	Cancel	
	wlan2	₹ \$	Apply	
Certificate:	none	₹	,	
Discovery Interfaces:		•		
	Lock To CAPsMAN			CAPsMAN Addresses należy
CAPsMAN Addresses:	10.31.31.1	\$		zmienić na swói
CAPsMAN Names:		\$		
CAPsMAN Certificate Common Names:		\$		
Bridge:	bridge-capsman	₹		
	Static Virtual			
Requested Certificate:				
Locked CAPsMAN Common Name:				

/interface wireless cap set bridge=bridge-capsman caps-man-addresses=10.31.31.1 enabled=yes interfaces=wlan1,wlan2

