

Podstawy
konfiguracji
Mikro-Tika

Copyright



202

Definicja Mikro-Tika:

- ▶ *Mikro-Tik to globalnie uznany producent sprzętu sieciowego i oprogramowania, który oferuje wszechstronne rozwiązania w dziedzinie komunikacji sieciowej.*

Główne aplikacje Mikro-Tika:

- ▶ *Router*
- ▶ *Access Point*
- ▶ *Firewall*
- ▶ *VPN (Virtual Private Network)*
- ▶ *Proxy serwer*

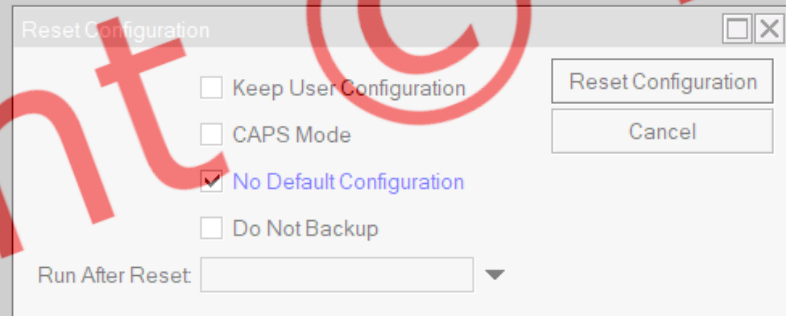
2024



COPYRIGHT

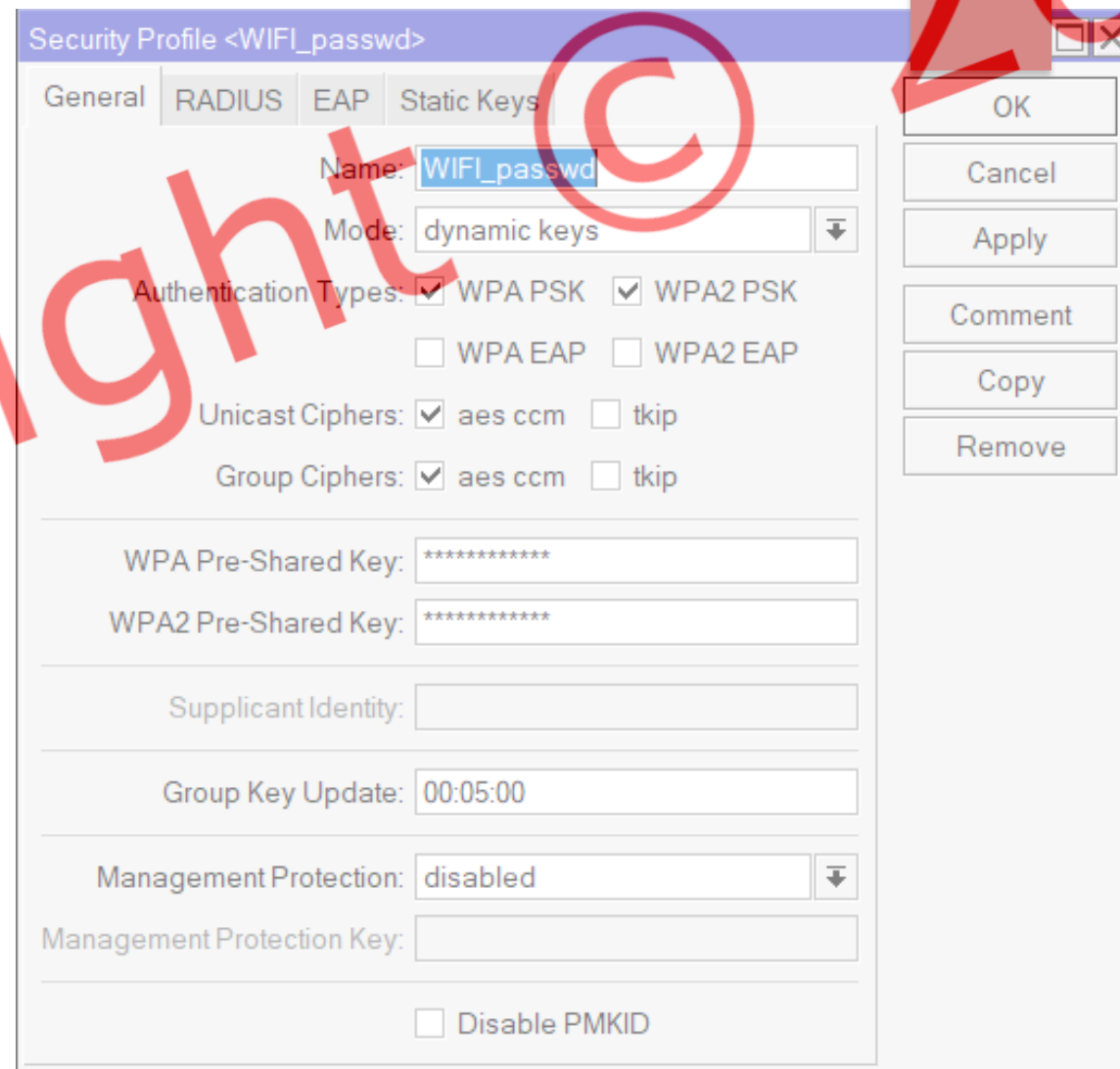
Przykład konfiguracji:

Aby prawidłowo zacząć konfigurację routera należy połączyć się z nim przy użyciu aplikacji WinBox oraz przywrócić go do domyślnej konfiguracji. W tym celu w zakładce: "system -> reset configuration" zaznaczamy opcje jak na zrzucie ekranu obok i potwierdzamy reset.



Konfiguracja będzie polegać na odebraniu przez Mikro-Tika sygnału WiFi z innego routera co umożliwi zrobienie punktu dostępowego bez potrzeby łączenia urządzeń skrętkami.

W tym celu w zakładce "interfaces" uruchamiamy nasze zdalne połączenie zaznaczając wlan1 oraz klikając przycisk "enable". Aby połączenie mogło działać potrzebujemy utworzyć security profile w zakładce "Wireless -> Security Profiles" tworzymy nowy profil, w polach Wpa pre-Shared Key oraz Wpa2 pre-Shared Key wpisujemy hasło do sieci WiFi, z która będziemy chcieli się połączyć.

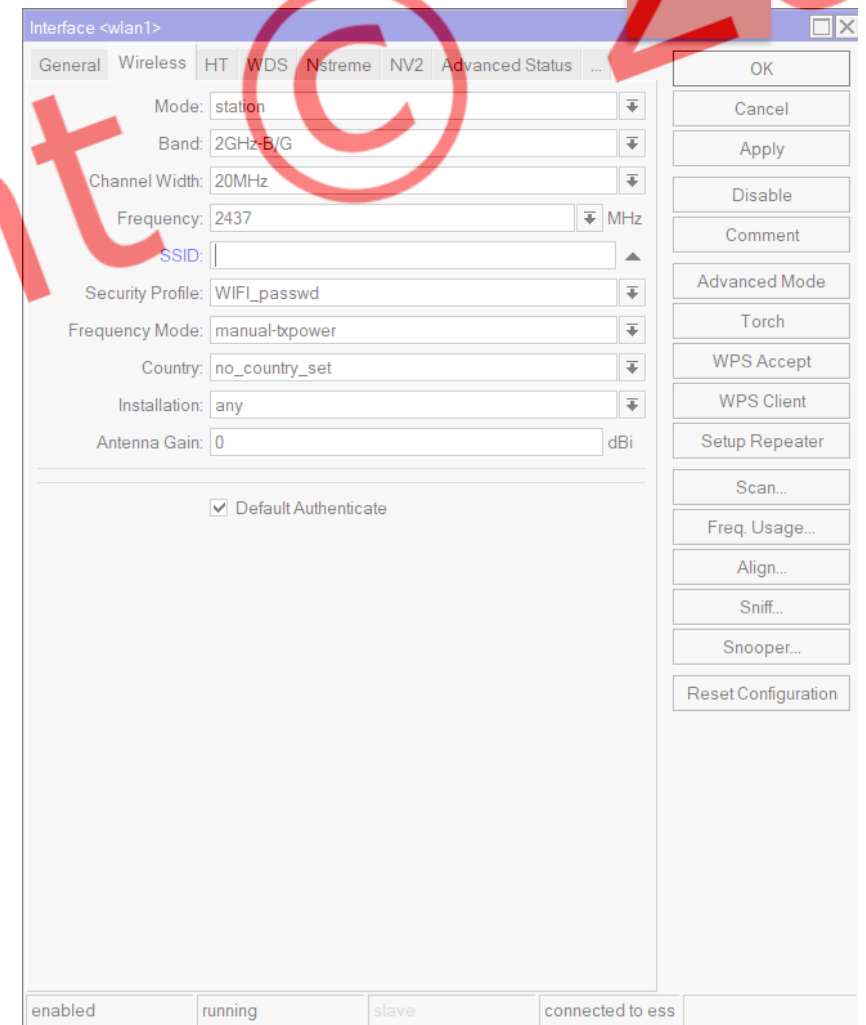


The screenshot shows the Mikrotik configuration window for a Security Profile named "WIFI_passwd". The window has several tabs: "General", "RADIUS", "EAP", and "Static Keys". The "General" tab is active. The configuration includes the following fields and options:

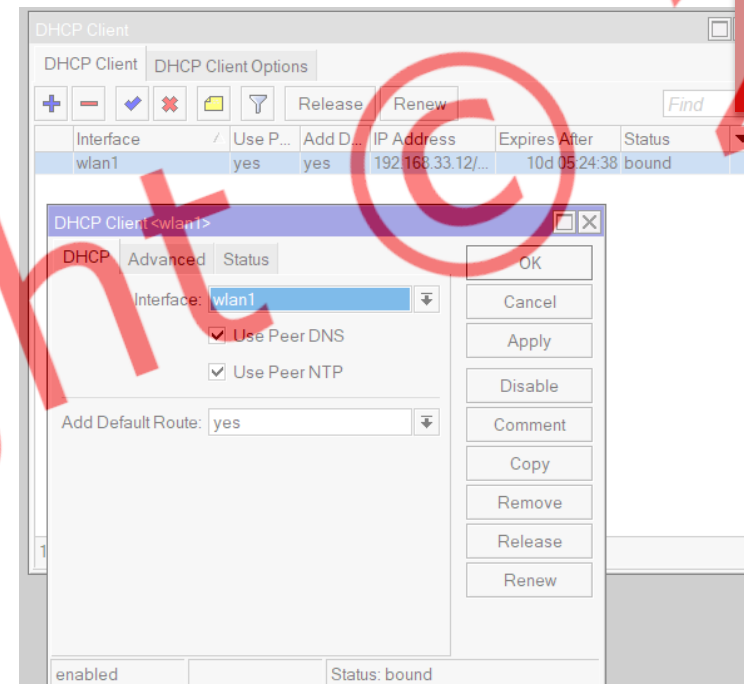
- Name:** WIFI_passwd
- Mode:** dynamic keys
- Authentication Types:** WPA PSK, WPA2 PSK, WPA EAP, WPA2 EAP
- Unicast Ciphers:** aes ccm, tkip
- Group Ciphers:** aes ccm, tkip
- WPA Pre-Shared Key:** [masked]
- WPA2 Pre-Shared Key:** [masked]
- Supplicant Identity:** [empty]
- Group Key Update:** 00:05:00
- Management Protection:** disabled
- Management Protection Key:** [empty]
- Disable PMKID

On the right side of the window, there are buttons for "OK", "Cancel", "Apply", "Comment", "Copy", and "Remove". A large red watermark "Copyright © 2022" is overlaid on the image.

Następnie w zakładce "interfaces -> 2-krotnie klikamy na wlan1 -> WireLess" ustawiamy mode na station, oraz klikamy scan, szukamy sieci klikając "start" oraz wybieramy naszą sieć, od której uzyskamy dostęp do internetu. W polu SSID powinna znajdować się nasza nazwa sieci. Kolejno w polu security profile wybieramy wcześniej utworzony profil z hasłem do naszej sieci.



Do prawidłowego działania potrzebujemy dodać klienta DHCP. W tym celu wchodzimy w "IP -> DHCP Client" oraz dodajemy klienta przyciskiem "+". Wybieramy interface jako wlan1 i zatwierdzamy "apply". W zakładce "Bridge" możemy utworzyć i skonfigurować mosty, a dodanie nowego mostu (na przykład "bridge1") pozwoli na działanie kilku portów ethernet w naszym routerze. W zakładce "bridge" dodajemy nowy most o nazwie bridge1. Następnie w zakładce ports dodajemy porty, które chcemy połączyć ze sobą (przykład na zrzucie ekranu).



#	Interface	Bridge	Horizon	Trusted	Priority (h...	Path Cost	Role	Root Path ...
0	H ether1	bridge1		no	80	10	designated port	
1	IH ether2	bridge1		no	80	10	disabled port	
2	IH ether3	bridge1		no	80	10	disabled port	
3	IH ether4	bridge1		no	80	10	disabled port	
4	IH wlan3	bridge1		no	80	10	designated port	

Aby WiFi na konfigurowanym routerze działało prawidłowo potrzebujemy wybrać w zakładce "Wireless -> Wifi interfaces" pole Setup Repeater uprzednio klikając w wlan1 oraz skonfigurować go w podany na rzucie ekranu obok sposob. SSID to nazwa naszej sieci, którą tworzymy, w polu Security Profile wybieramy wcześniej utworzony profil, dzięki czemu nasze hasło do sieci będzie identyczne jak do głównej.

Interface <wlan3>

General Wireless WDS Status Traffic

Mode: ap bridge

Secondary Channel:

SSID: DOMNET_1

Master Interface: wlan1

Security Profile: WIFI_passwd

WPS Mode: disabled

VLAN Mode: no tag

VLAN ID: 1

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

enabled running slave running ap

OK

Cancel

Apply

Disable

Comment

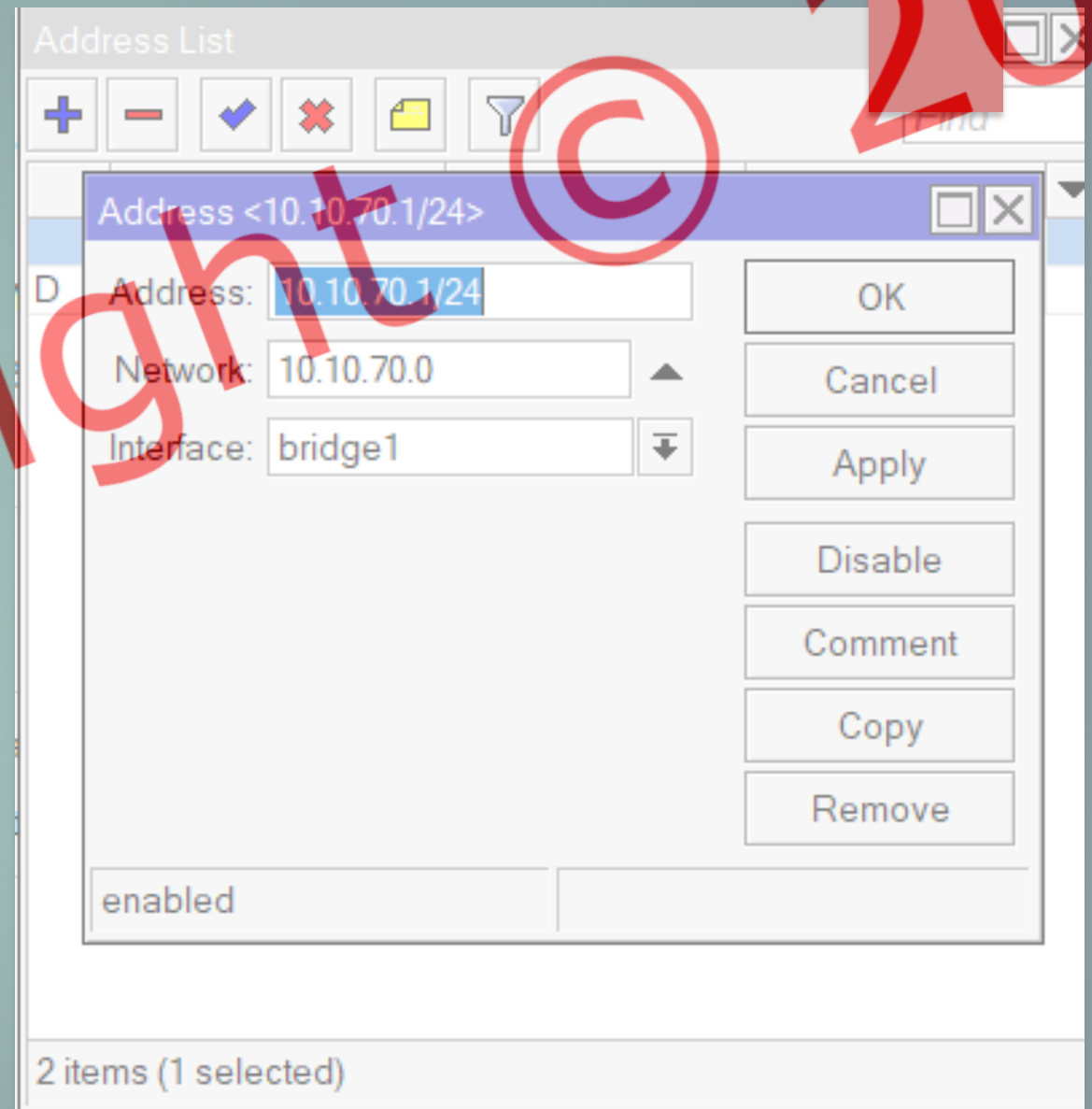
Copy

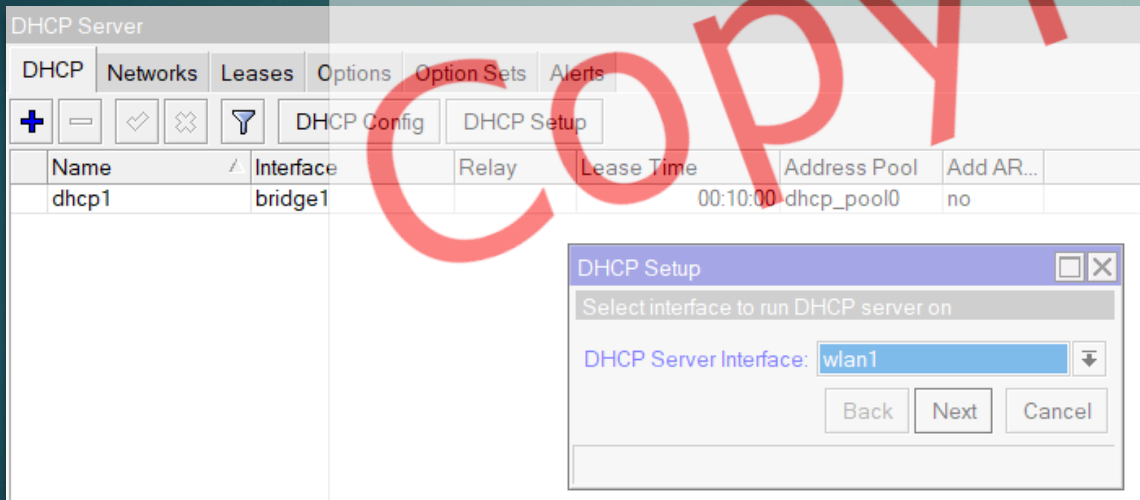
Remove

Advanced Mode

Torch

Następnie w zakładce "IP - > Addresses" w MikroTiku konfigurujemy adresy IP, które są przypisywane do poszczególnych interfejsów lub interfejsów wirtualnych urządzenia.

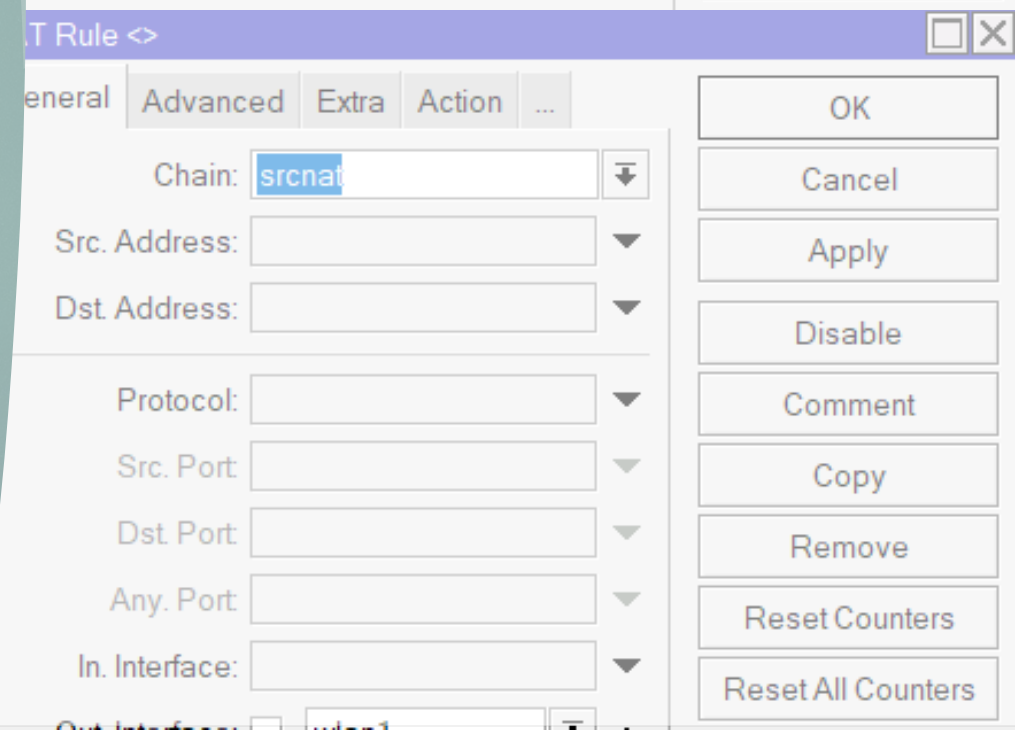
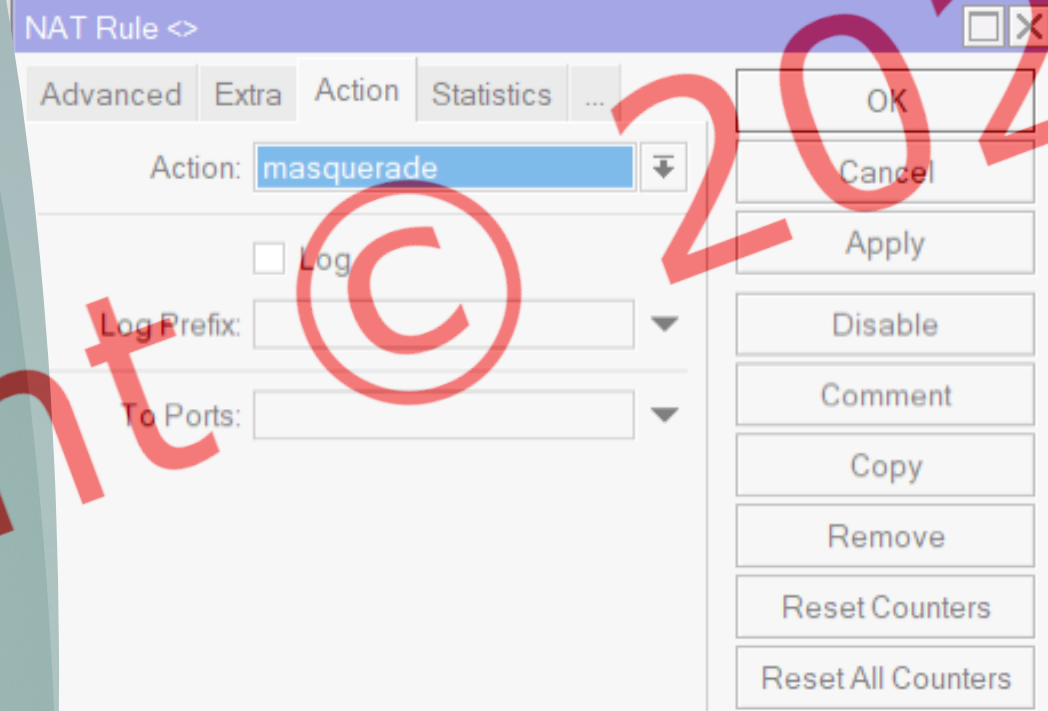





Kolejnym krokiem będzie utworzenie serwera DHCP w naszym routerze. Wybierając zakładkę "IP -> DHCP Server -> DHCP Setup" klikając next kilkukrotnie utworzymy serwer, dzięki któremu nasza sieć będzie automatycznie przydzielać adresy IP, maski podsieci, bramy urządzeniom podłączonym do sieci.

Ostatnim krokiem będzie utworzenie Firewalla. Utworzenie go jest kluczowym elementem zabezpieczania sieci i systemów przed nieautoryzowanym dostępem, atakami oraz innymi zagrożeniami. W tym celu w zakładce "IP -> Firewall -> NAT" dodajemy regułę jak na zrzutach obok.

Po skonfigurowaniu naszego Mikro-Tika próbujemy połączyć się z nim poprzez port ethernet (np. Laptopem) oraz WiFi (np. Telefonem). Jeśli sieć łączy się prawidłowo z obydwojema urządzeniami nasza konfiguracja działa.





MikroTik, jako narzędzie do zarządzania sieciami, oferuje nie tylko solidną konfigurację, ale także elastyczność, umożliwiając dostosowanie sieci do konkretnych potrzeb i wymagań. Wykorzystanie zakładek takich jak "Bridge", "Addresses" czy "Firewall" pozwala na efektywne kształtowanie ruchu w sieci, zabezpieczanie urządzeń oraz optymalizację komunikacji. Pamiętajmy, że MikroTik to nie tylko narzędzie dla profesjonalistów ds. sieci, ale także dostępne dla szerokiego grona użytkowników, którzy chcą skonfigurować swoją sieć zgodnie z indywidualnymi potrzebami. Warto kontynuować eksplorację możliwości, jakie oferuje MikroTik, aby nasze sieci były nie tylko bezpieczne, ale także efektywne i dostosowane do rosnących wymagań dzisiejszych czasów.

2024

Copyright © 2022

Dziękuję za
uwagę

MARCIN SERAFIN