



KONFIGURACJA SIECI WLAN

Tytuł: Konfiguracja sieci WLAN
Autor: Jakub Niewiadomski
Redaktor merytoryczny: Piotr Chojnacki

O autorach:

Jakub Niewiadomski

Uczeń profilu technik informatyk. Pasjonat programowania i sieci komputerowych (ukończony kurs CCNA), a hobbystycznie związany również z fotografią koncertową, gitarą oraz instrumentami klawiszowymi.

Piotr Chojnacki

Nauczyciel przedmiotów zawodowych informatycznych. Wieloletni koordynator projektów informatycznych i współpracy cyfrowej z uczelniami wyższymi i instytucjami. Właściciel firmy szkoleniowej z zakresu IT. Instruktor CISCO CCNA R&S, CCNA Security, CCNP. Egzaminator i szkoleniowiec ECDL. Współrealizator projektów unijnych dotyczących zdobywania kompetencji ICT i TIK.



Ministerstwo
Cyfryzacji

Program OSE powstał dzięki staraniom Ministerstwa Cyfryzacji.

NASK

Operatorem OSE jest NASK Państwowy Instytut Badawczy.

Streszczenie

W wykładzie omówione zostały informacje dotyczące teorii działania sieci bezprzewodowych oraz przykładowa konfiguracja punktu dostępu w oparciu o narzędzie CAPsMAN. Do pełnego zrozumienia zawartego materiału niezbędna jest podstawowa wiedza o funkcjonowaniu sieci komputerowych, zawarta w kursie „Konfiguracja sieci oraz urządzeń do poprawnego działania”.

Poruszone zostały zagadnienia dotyczące standardów sieci WLAN, wykorzystywanych urządzeń, technologii Power-over-Ethernet, topologii sieci bezprzewodowych, rodzajów tych sieci, szyfrowań połączeń oraz podstaw bezpieczeństwa. W części praktycznej zamieszczono opis przykładowej konfiguracji routera oraz punktu dostępowego firmy Mikrotik.

Zeszyt ćwiczeń powstał w celu przejrzystego zaprezentowania najważniejszych informacji dotyczących sieci bezprzewodowych, umożliwienia poszerzenia posiadanej wiedzy oraz nabycia dodatkowych umiejętności praktycznych.

Spis treści

Wykład	5
Wprowadzenie do sieci bezprzewodowych	5
Czym jest WLAN?	5
Wykorzystywane standardy	5
Jakie elementy składają się na infrastrukturę sieciową?	5
PoE	6
Topologie	6
Rodzaje sieci bezprzewodowych	7
Szyfrowanie	7
Filtrowanie adresów MAC	8
Izolacja klientów	8
Wady i zalety sieci WLAN	8
Warsztaty	9
Konfiguracja sieci bezprzewodowej w oparciu o narzędzie CAPsMAN	9
Wykorzystane urządzenia	9
Przystosowanie AP do pracy pod kontrolą CAPsMAN	9
Konfiguracja routera do pracy jako CAPsMAN manager	12
Źródła	22

Wykład

Wprowadzenie do sieci bezprzewodowych

Czym jest WLAN?

WLAN, jest to bezprzewodowa wersja sieci LAN. Skrót ten pochodzi od terminu Wireless LAN, czyli sieci bez użycia przewodów, gdzie medium transmisyjnym jest komunikacja radiowa. Dwa najczęściej stosowane pasma to 2.4GHz oraz 5GHz.

Wykorzystywane standardy

W sieciach WLAN jest wykorzystywana rodzina standardów IEEE 802.11. Kolejne wersje standardów ewoluują pod kątem wzrostu szybkości przesyłu danych. Obecnie najczęściej spotykanymi na rynku są rozwiązania oparte na standardach IEEE 802.11n i IEEE 802.11ac.

Standard	Częstotliwość	Szerokość pasma	Maksymalna teoretyczna prędkość przesyłu	Maksymalny teoretyczny zasięg
802.11	2.4 GHz	20 MHz	2 Mbps	20 m
b	2.4 GHz	21 MHz	11 Mbps	35 m
a	5 GHz	22 MHz	54 Mbps	35 m
G	2.4 GHz	23 MHz	54 Mbps	70 m
N	2.4 GHz, 5 GHz	24 MHz oraz 40 MHz	600 Mbps	70 m
Ac	5 GHz	20, 40, 80, 80+80=160 MHz	6,93 Gbps	35 m
Ad	60 GHz	2.16 GHz	6,76 Gbps	10 m
af	54-790 MHz	6, 7, 8 MHz	26,7 Mbps	> 1km
ah	900 MHz	1, 2, 4, 8, 16 MHz	40 Mbps	1 km

Jakie elementy składają się na infrastrukturę sieciową?

Na infrastrukturę fizyczną sieci składają się m.in. następujące elementy:

1. Bezprzewodowa karta sieciowa – odbiornik danych z sieci bezprzewodowej, działa niemal identycznie jak przewodowa karta sieciowa;
2. Punkt dostępowy (AP – Access Point) – umożliwia rozszerzenie działania naszej sieci o bezprzewodowy dostęp do niej. Urządzenie AP posiada przynajmniej dwa interfejsy sieciowe, tj. port sieci Ethernet, zazwyczaj odpowiadający za połączenie z siecią lokalną, która zapewnia komunikację z siecią lokalną oraz interfejs bezprzewodowy odpowiadający za działanie WLAN.
3. Antena – jej zadaniem jest prawidłowa propagacja fal radiowych, umożliwiającą zwiększenie zasięgu czy ukierunkowanie go. Dzięki właściwemu doborowi anteny możemy uzyskać prawidłowe pokrycie sygnałem radiowym planowanego obszaru.

PoE

Ważnym elementem technicznym sieci bezprzewodowej jest obecność technologii Power over Ethernet IEEE 802.3af. Jest to technologia umożliwiająca zasilanie urządzenia sieciowe poprzez wieloparowe kable miedziane (skrętkę). Jest to niezwykle wygodne rozwiązanie, ze względu na potrzebę doprowadzenia do urządzenia wyłącznie przewodu sieciowego, w którym będzie również napięcie – nie musimy się martwić o dostęp do zasilania w okolicy urządzenia. Wyróżniamy dwa typy PoE:

- Pasywne – dostarcza do urządzenia ciągle stałe napięcie;
- Aktywne – komunikuje się z urządzeniem i dostosowuje napięcie do jego potrzeb.

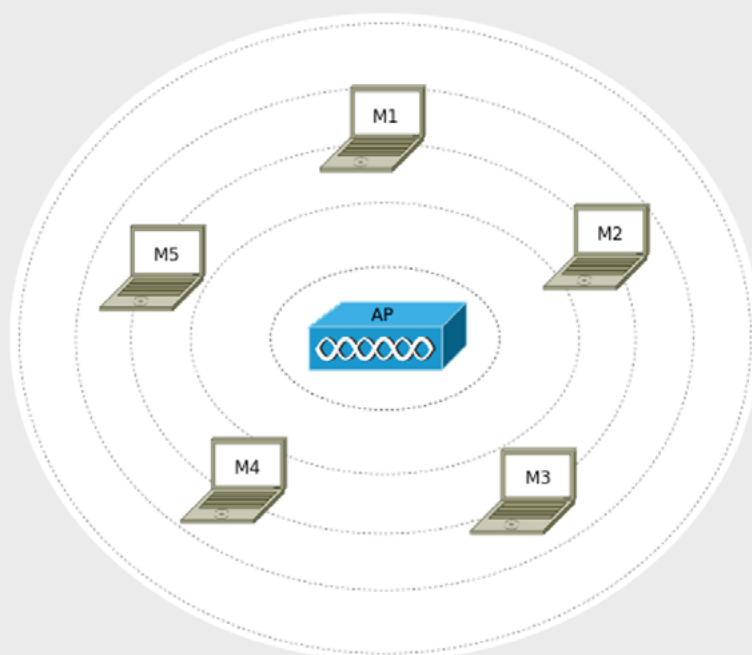
W wypadku gdy do złącza PoE aktywnego zostanie podłączone urządzenie nie wykorzystujące tej technologii, zasilanie zostanie po prostu wyłączone na tym porcie. W przypadku podłączenia dowolnego urządzenia do portu pasywnego, zasilanie przez cały czas będzie włączone. Podłączenie urządzenia nie wykorzystującego PoE do gniazda, w którym działa pasywne PoE, może skutkować uszkodzeniem karty sieciowej oraz innych podzespołów urządzenia!

Topologie

Sieci bezprzewodowe pokrywające założony obszar są zazwyczaj budowane w oparciu o dwie topologie: gwiazdy i kraty.

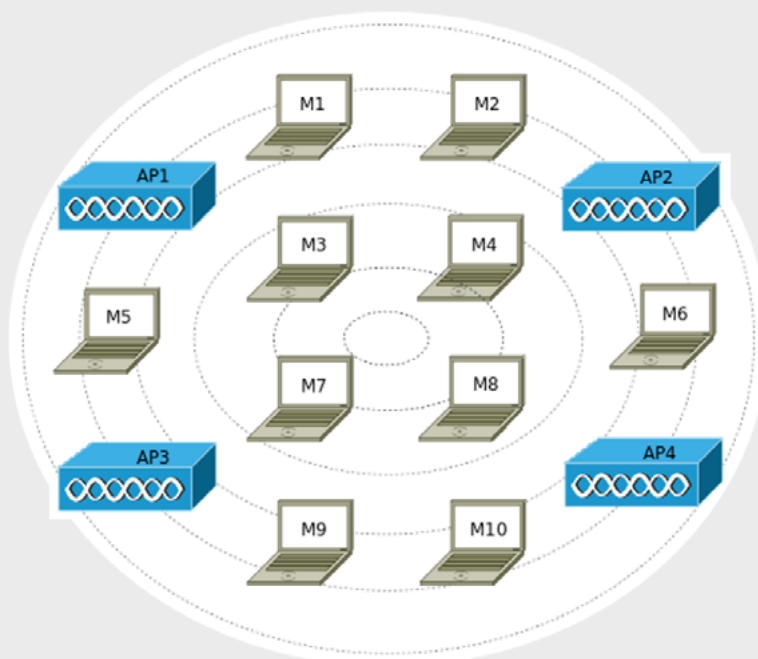
Topologia gwiazdy

Wykorzystuje jeden centralny punkt dostępu jako serce sieci, przy ułożeniu np. stacji roboczych dookoła niego.



Topologia kraty

Charakteryzuje ją bezpośrednia komunikacja ze sobą wszystkich punktów dostępowych. Kratownica poprawia pokrycie obszaru sygnałem, zwiększa wydajność i niezawodność działania. Ze względu na większą ilość stosowanych urządzeń, krata jest rozwiązaniem droższym.



Rodzaje sieci bezprzewodowych

Ad-hoc

Cechą tego rodzaju sieci jest bezpośrednia komunikacja urządzeń ze sobą. Porozumiewanie się tych urządzeń jest uzyskane z pominięciem punktów dostępu - komputer stacjonarny lub urządzenie przenośne mogą komunikować się ze sobą bezpośrednio.

Infrastruktura

Tego rodzaju sieć jest przeciwieństwem Ad-hoc, ponieważ cała komunikacja opiera się na punktach dostępowych.

Szyfrowanie

W sieciach bezprzewodowych możemy spotkać wiele zabezpieczeń pozwalających nam uchronić je przed niepowołanym dostępem osób trzecich.

Najważniejszym szyfrowaniem jest WPA2. Jest to standard szyfrowania, który obecnie generuje najcięższy do złamania klucz wspomagany przez dodatkowe technologie, których celem jest ochrona naszej sieci. Szyfrowanie to charakteryzuje się także ogromną bazą danych, której zawartość wypełniają zabezpieczenia przeciwko błędom spostrzeżonym w poprzednich wersjach szyfrowania dostępu do sieci bezprzewodowych.

Filtrowanie adresów MAC

Filtrowaniem nazywamy wybranie interesujących nas w tym przypadku adresów. Filtrowanie jest swego rodzaju sitem, które pozwala lub zabrania konkretnym adresom MAC dostępu do sieci bezprzewodowej.

Izolacja klientów

Izolacja klientów jest zabezpieczeniem w szczególności sieci z większymi ilościami użytkowników. Jest to opcja bezpieczeństwa nie pozwalająca użytkownikom sieci bezprzewodowej na komunikację ze sobą. Jest najczęściej stosowana w sieciach publicznych/hotspotach: restauracjach, komunikacji miejskiej etc.

Wady i zalety sieci WLAN

Zalety

- Łatwość instalacji z powodu braku okablowania urządzeń końcowych, podłączenia wymaga wyłącznie punkt dostępowy;
- Elastyczny zasięg pokrycia sygnałem mogący przybierać różny zakres odległości;
- Szybka rozbudowa i modyfikacja struktury sieci.

Wady

- Podatność na zakłócenia sygnału
- Mniejsza stabilność połączenia w porównaniu z siecią przewodową

Warsztaty

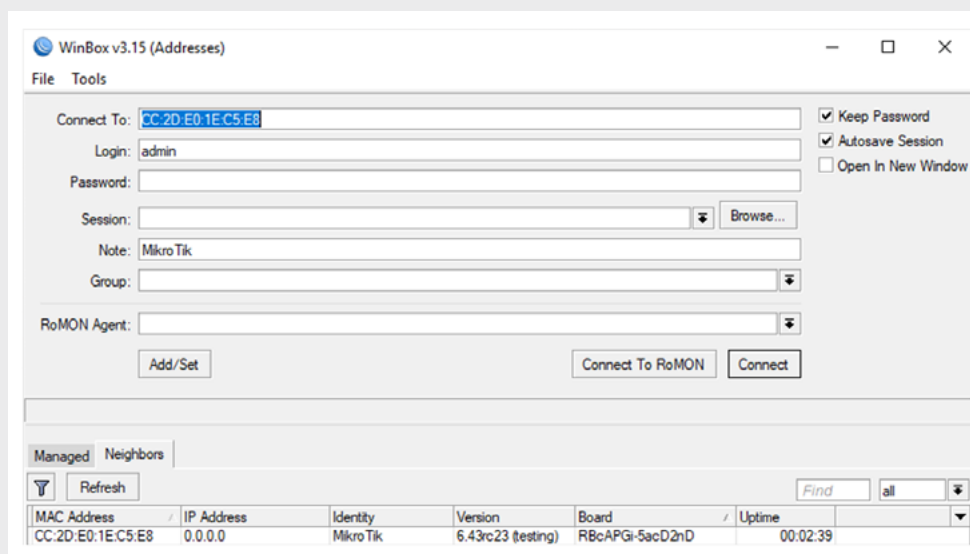
Konfiguracja sieci bezprzewodowej w oparciu o narzędzie CAPsMAN

Wykorzystane urządzenia

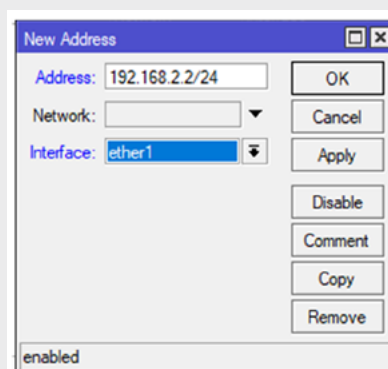
Do wykonania opisanej niżej konfiguracji niezbędny jest router firmy Mikrotik obsługujący narzędzie CAPsMAN oraz dowolny punkt dostępu z oferty tej firmy – w naszym wypadku jest to model dwuzakresowy.

Przystosowanie AP do pracy pod kontrolą CAPsMAN

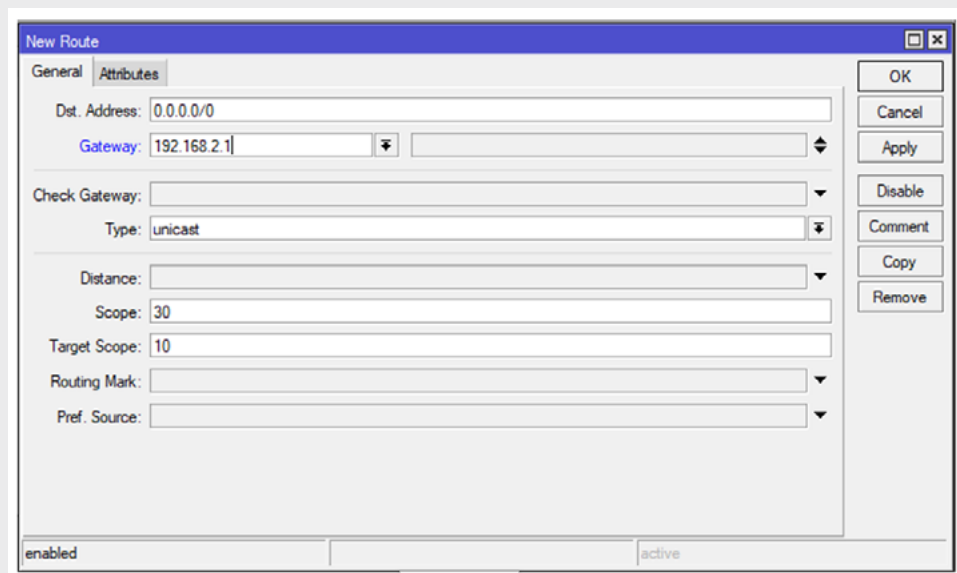
Na początek podłączamy AP bezpośrednio do przewodowej karty sieciowej. Uruchamiamy oprogramowanie winbox, przechodzimy do zakładki neighbors, klikamy przycisk refresh do momentu, aż pojawi się nasze urządzenie. Klikamy dwukrotnie na jego MAC Address, w polu Login admin, password puste, connect.



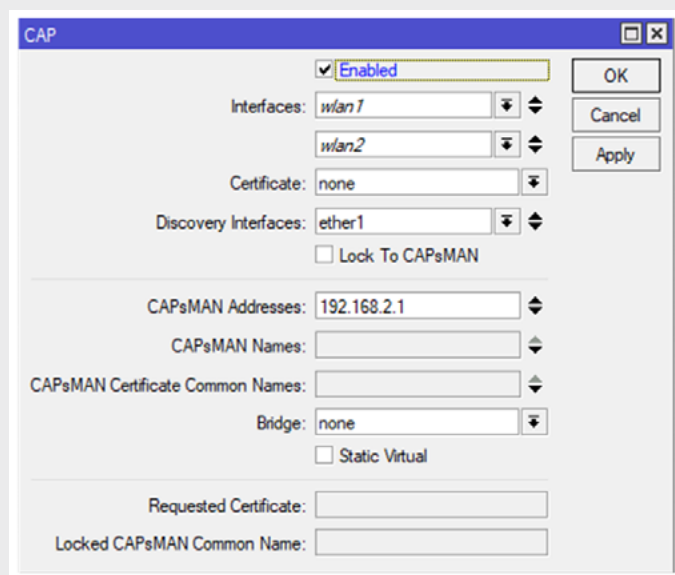
Wchodzimy do zakładki IP -> Addresses i dodajemy adres 192.168.2.2/24 dla portu ether 1 - będzie to adres IP naszego routera.



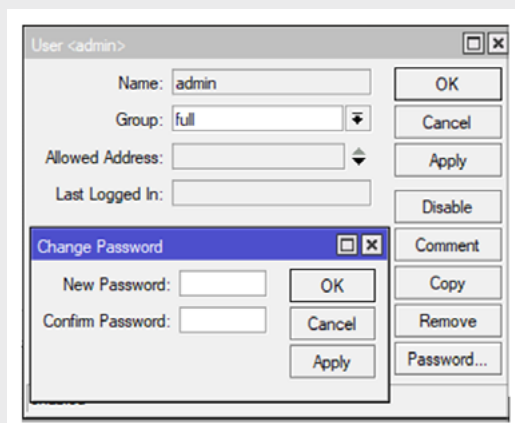
Ze względu na to, że ustaliliśmy statyczny adres, musimy również dokonać odpowiedniego trasowania, w tym celu wchodzimy do zakładki IP -> Routes i dodajemy nową trasę domyślną (0.0.0.0/0) przez bramę 192.168.2.1



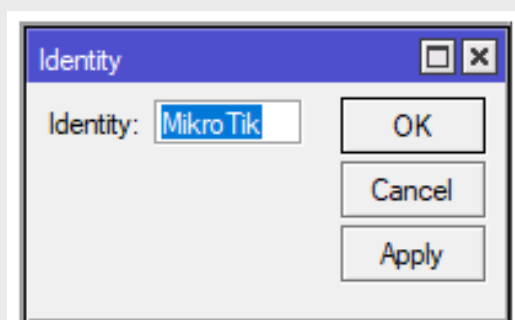
Teraz wchodzimy do zakładki Wireless, następnie klikamy przycisk CAP. Wybieramy następujące opcje: Enabled, Interfaces: dodajemy oba interfejsy wlan, Discovery Interfaces: ether1, CAPsMAN Addresses: 192.168.2.1



Teraz, aby uniknąć nieautoryzowanego dostępu, zmieniamy domyślne (puste) hasło użytkownika admin na bezpieczne hasło. W tym celu przechodzimy do zakładki System -> Users, klikamy dwukrotnie na użytkownika admin, następnie przycisk Password i wpisujemy nowe hasło.



Zmienimy również nazwę naszego routera, by łatwo odnaleźć go pośród pozostałych urządzeń mikrotik w sieci (każde z nich ma nazwę domyślną MikroTik). W tym celu wchodzimy do zakładki System -> Identity i wpisujemy nazwę AP1.

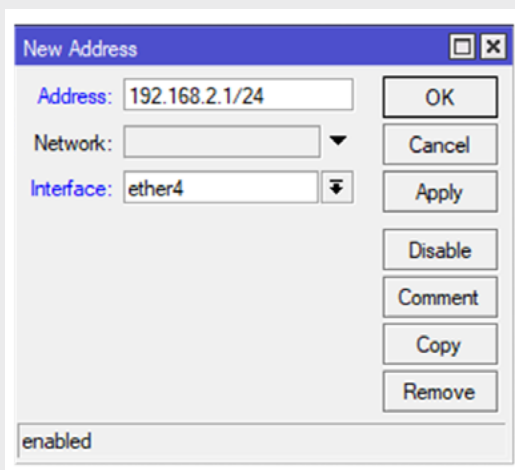


Teraz podłączamy punkt dostępu do któregoś z wolnych portów naszego routera - w tym wypadku będzie to ether4.t

Konfiguracja routera do pracy jako CAPsMAN manager

Ponownie poprzez oprogramowanie WinBox łączymy się (tym razem) z naszym routerem, którego aktualna konfiguracja pochodzi z kursu o tworzeniu sieci LAN.

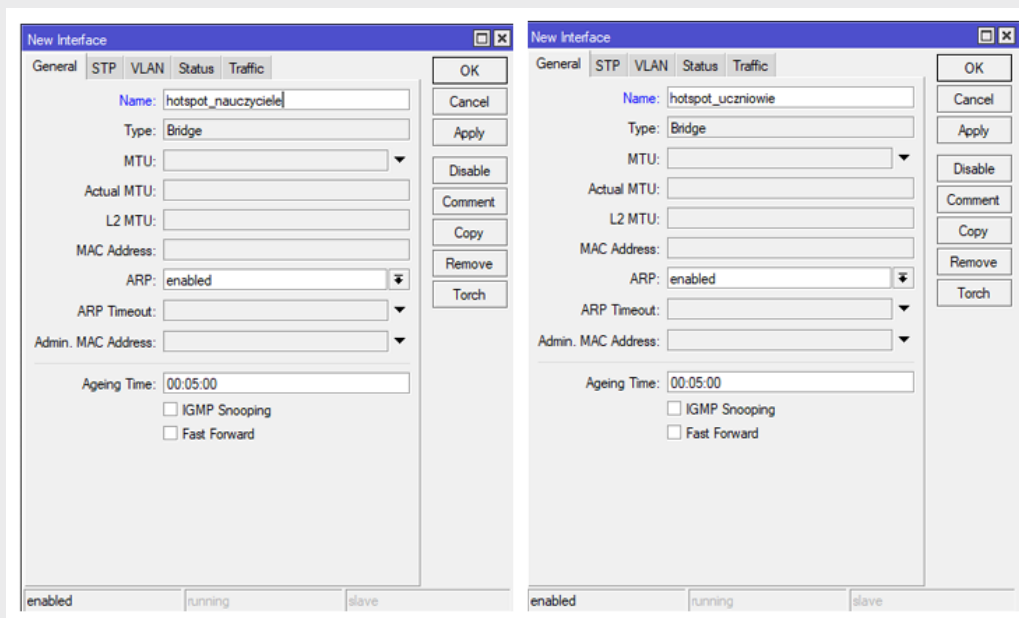
Wchodzimy do zakładki IP -> Addresses i dodajemy nowe, statyczne ip 192.168.2.1/24 dla portu, do którego podłączyliśmy AP (ether4).



The 'New Address' dialog box shows the following configuration:

- Address: 192.168.2.1/24
- Network: (empty dropdown)
- Interface: ether4
- Status: enabled
- Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

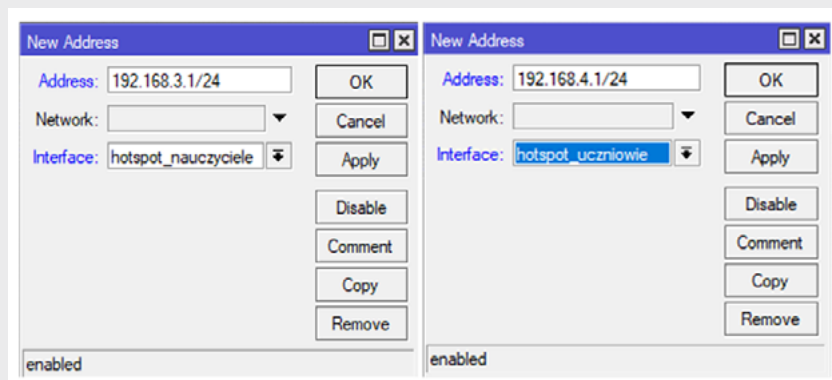
Przechodzimy teraz do zakładki bridge i tworzymy nowe mosty dla hotspotów: nauczycieli i uczniów.



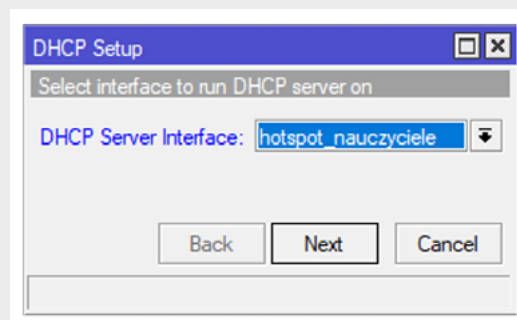
The 'New Interface' dialog box shows the following configuration for both interfaces:

- Name: hotspot_nauczyciele (left) / hotspot_uczniowie (right)
- Type: Bridge
- MTU: (empty dropdown)
- Actual MTU: (empty text box)
- L2 MTU: (empty text box)
- MAC Address: (empty text box)
- ARP: enabled
- ARP Timeout: (empty dropdown)
- Admin. MAC Address: (empty dropdown)
- Ageing Time: 00:05:00
- IGMP Snooping: ☐
- Fast Forward: ☐
- Status: enabled
- Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch

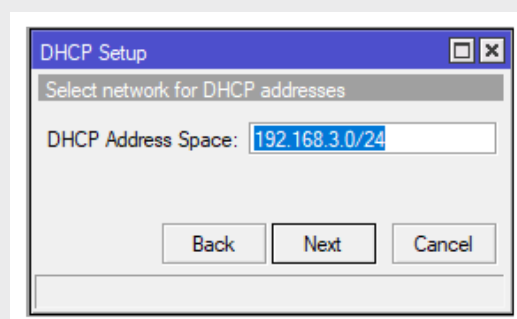
Teraz powracamy do zakładki IP -> Addresses i dodajemy adresy do tych mostów. Będą to: 192.168.3.1/24 oraz 192.168.4.1/24 .



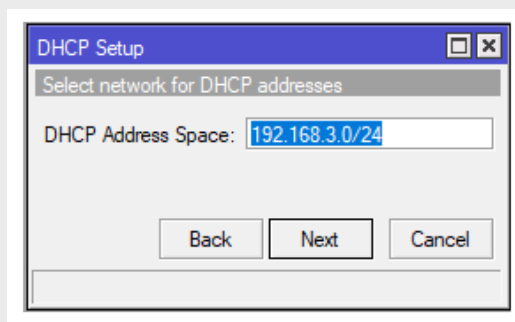
Musimy teraz uruchomić serwer DHCP dla obu tych mostów. Przechodzimy więc do zakładki IP -> DHCP Server i klikamy DHCP Setup. Wybieramy jako interfejs nasz most.



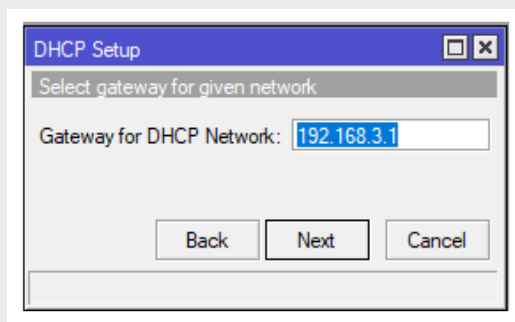
Przestrzeń adresowa została ustalona na podstawie ustawionego adresu w zakładce IP -> Addresses - pozostawiamy bez zmian.



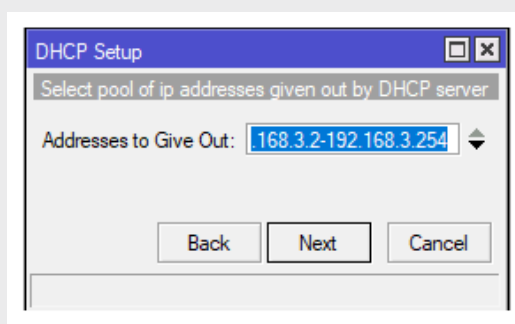
Brama domyślna, podobnie jak przestrzeń adresowa, również została ustalona automatycznie - jest to adres IP naszego routera dla danego mostu, pozostawiamy bez zmian.



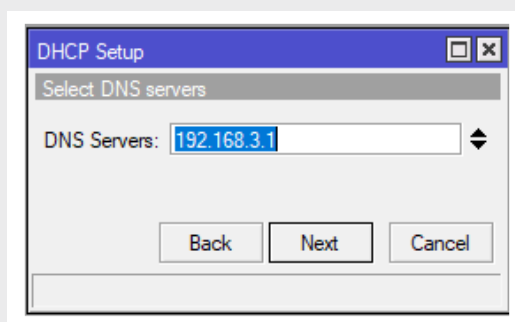
Zakres adresów, również bazowany na podstawie adresu ustalonego w IP -> Addresses i maski podsieci - pozostawiamy bez zmian.



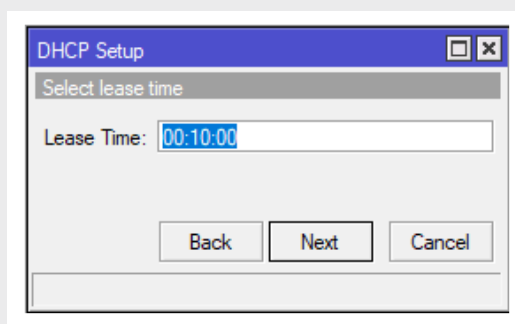
Zakres adresów, również bazowany na podstawie adresu ustalonego w IP -> Addresses i maski podsieci - pozostawiamy bez zmian.



Serwer DNS - wykorzystujemy uruchomioną na routerze usługę DNS, która dostępna jest pod adresem IP naszego routera dla danego mostu (taki sam jak brama domyślna).

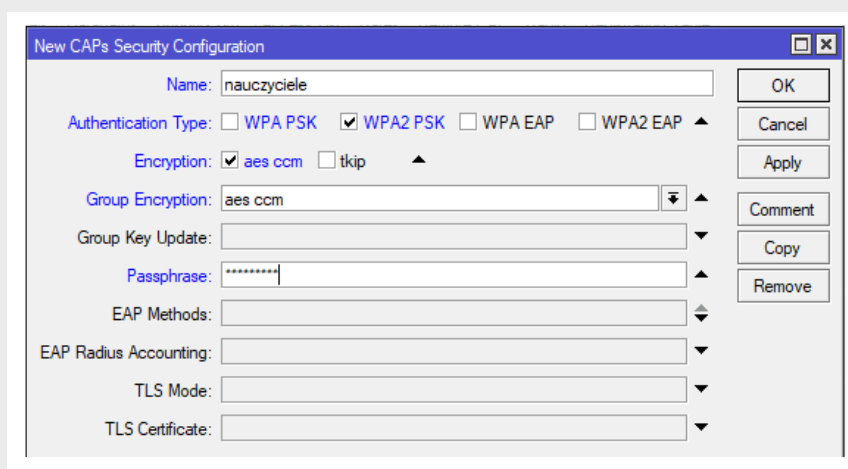


Czas leasingu, czyli przypisania adresu IP przez serwer DHCP do konkretnego urządzenia, również możemy pozostawić na domyślnej wartości 10 minut.



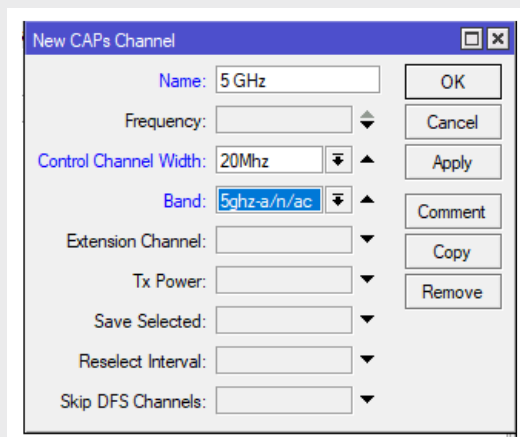
W podobny sposób konfigurujemy również DHCP dla drugiego mostu.

Przechodzimy teraz do konfiguracji CAPsMAN'a, czyli zakładka o tej samej nazwie. Zaczniemy od konfiguracji profilu zabezpieczeń - zakładka Security Cfg. Dodajemy nową konfigurację. Nazywamy ją nauczyciele, wybieramy WPA2 PSK oraz szyfrowanie AES CCM (zarówno indywidualne, jak i grupowe) oraz wpisujemy bezpieczne hasło.



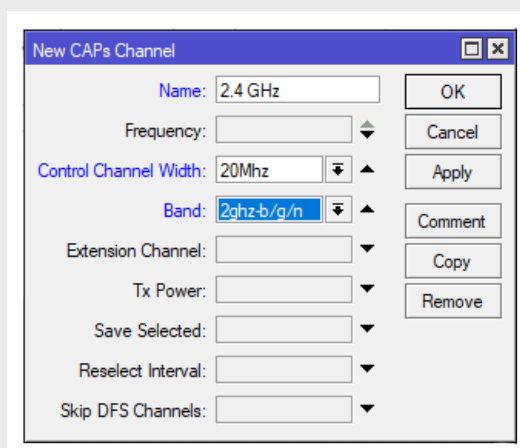
Czynność powtarzamy analogicznie dla uczniów.

Teraz przechodzimy do zakładki Channels, gdzie ustawimy wszystkie szczegóły związane z kanałami i nadawaniem. Dodajemy nową konfigurację o nazwie 5 GHz. Ustawiamy wyłącznie szerokość kanału - 20 MHz oraz pasmo 5ghz-a/n/ac.



The screenshot shows a 'New CAPs Channel' dialog box. The 'Name' field is set to '5 GHz'. The 'Frequency' field is empty. The 'Control Channel Width' is set to '20Mhz'. The 'Band' is set to '5ghz-a/n/ac'. The 'Extension Channel' is empty. The 'Tx Power' is empty. The 'Save Selected' is empty. The 'Reselect Interval' is empty. The 'Skip DFS Channels' is empty. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and 'Remove'.

Podobnie tworzymy kolejną o nazwie 2.4 GHz, szerokość kanału 20 MHz i pasmo 2ghz-b/g/n.



The screenshot shows a 'New CAPs Channel' dialog box. The 'Name' field is set to '2.4 GHz'. The 'Frequency' field is empty. The 'Control Channel Width' is set to '20Mhz'. The 'Band' is set to '2ghz-b/g/n'. The 'Extension Channel' is empty. The 'Tx Power' is empty. The 'Save Selected' is empty. The 'Reselect Interval' is empty. The 'Skip DFS Channels' is empty. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and 'Remove'.

Przechodzimy do kolejnej zakładki -> Datapaths i dodajemy nową. Nazywamy ją nauczyciele, wybieramy most (bridge) nauczycieli oraz zaznaczamy opcję client to client forwarding - gdy jest zaznaczona, wyłączona jest izolacja klientów.

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:

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

Podobnie dodajemy kolejną ścieżkę o nazwie uczniowie, most uczniów oraz odznaczamy opcję client to client forwarding.

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:

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

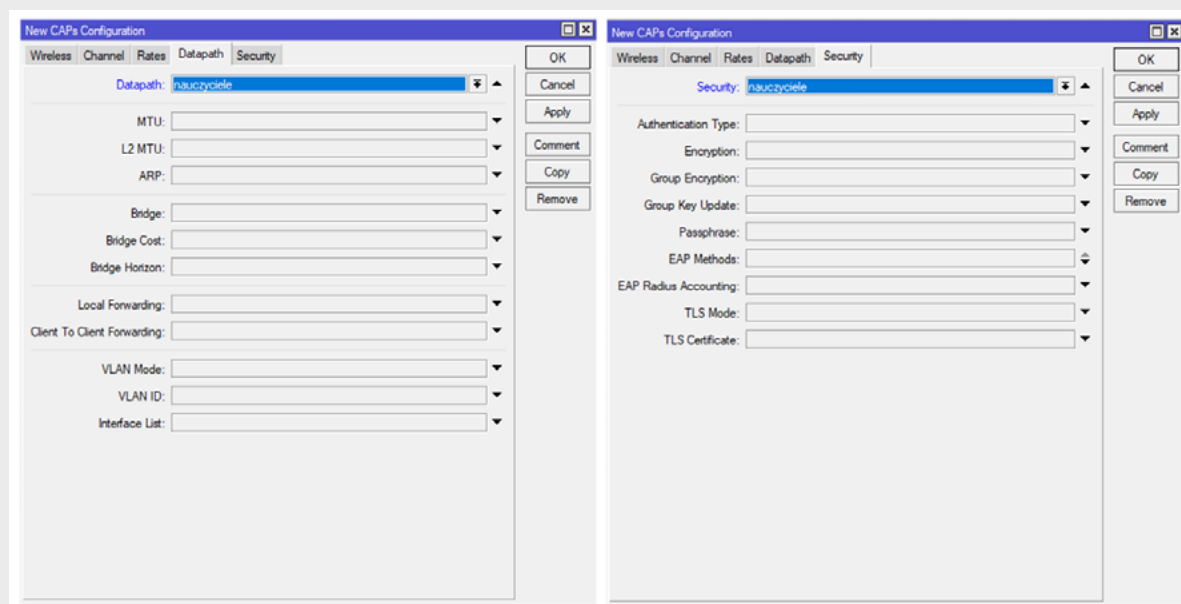
Przechodzimy do zakładki configurations. Dodajemy nową o nazwie nauczyciele 2.4, Mode: ap, SSID: Nauczyciele_2.4.

The screenshot shows the 'New CAPs Configuration' dialog box with the 'Wireless' tab selected. The 'Name' field is set to 'Nauczyciele 2.4', 'Mode' is set to 'ap', and 'SSID' is set to 'Nauczyciele_2.4'. Other fields like 'Hide SSID', 'Load Balancing Group', 'Distance', 'Hw. Retries', 'Hw. Protection Mode', 'Frame Lifetime', 'Disconnect Timeout', 'Keepalive Frames', 'Country', 'Max Station Count', 'Multicast Helper', 'HT Tx Chains', 'HT Rx Chains', and 'HT Guard Interval' are all empty. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and 'Remove'.

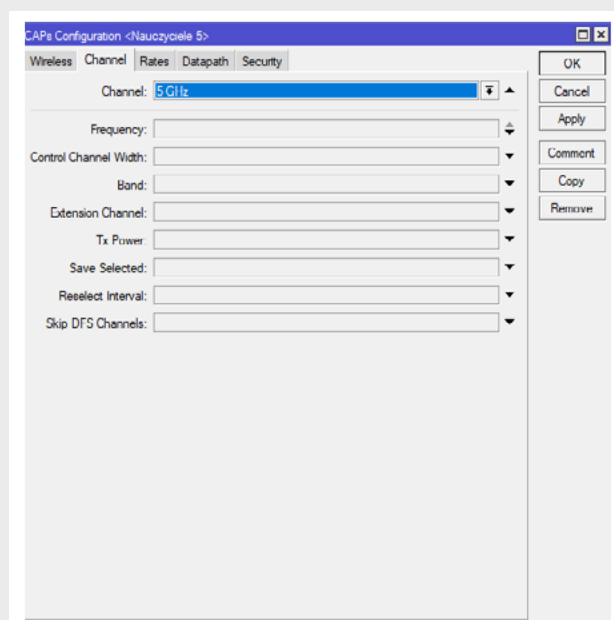
W zakładce Channel wybieramy predefiniowane ustawienia z pola Channel dla 2.4 GHz (które wcześniej utworzyliśmy) - parametry nie uwzględnione w tej predefiniowanej konfiguracji zostaną dobrane automatycznie.

The screenshot shows the 'New CAPs Configuration' dialog box with the 'Channel' tab selected. The 'Channel' dropdown menu is set to '2.4 GHz'. Other fields like 'Frequency', 'Control Channel Width', 'Band', 'Extension Channel', 'Tx Power', 'Save Selected', 'Reselect Interval', and 'Skip DFS Channels' are all empty. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and 'Remove'.

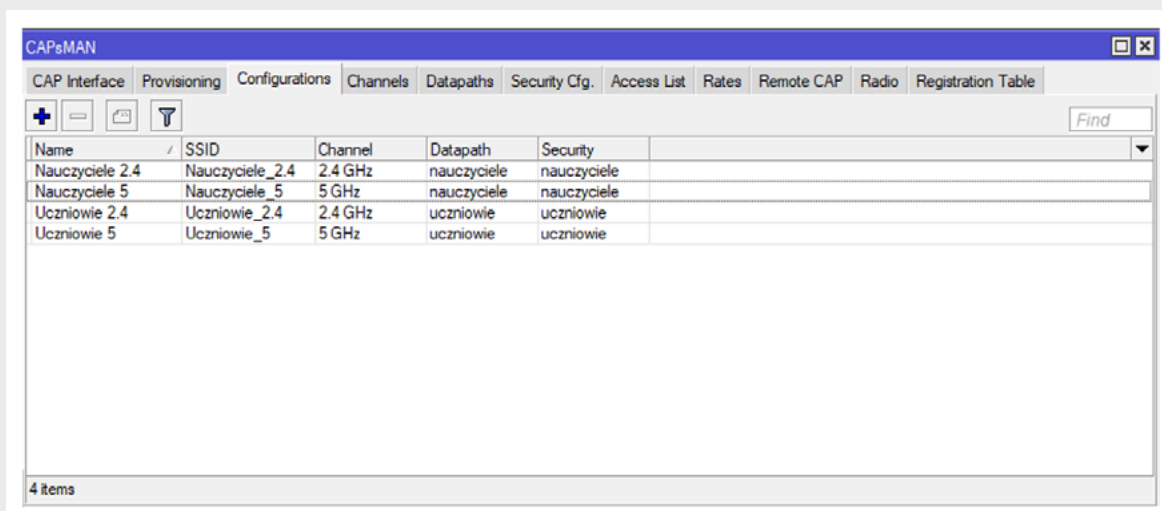
W zakładkach datapath i security wybieramy również predefiniowane konfiguracje nauczyciele.



Podobnie dodajemy kolejną konfigurację o nazwie nauczyciele 5, Mode: ap, SSID: Nauczyciele_5. W zakładce Channel wybieramy predefiniowane ustawienia z pola Channel dla 5 GHz. Pozostałe zakładki konfigurujemy jak w poprzedniej konfiguracji.



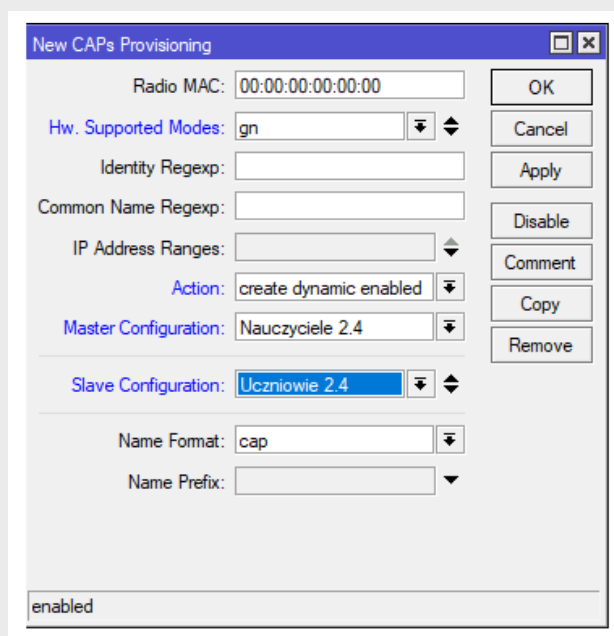
Analogicznie wykonujemy konfigurację dla uczniów. Powinniśmy otrzymać 4 konfiguracje, tak jak na poniższym zrzucie.



Name	SSID	Channel	Datapath	Security
Nauczyciele 2.4	Nauczyciele_2.4	2.4 GHz	nauczyciele	nauczyciele
Nauczyciele 5	Nauczyciele_5	5 GHz	nauczyciele	nauczyciele
Uczniowie 2.4	Uczniowie_2.4	2.4 GHz	uczniowie	uczniowie
Uczniowie 5	Uczniowie_5	5 GHz	uczniowie	uczniowie

4 items

Teraz w zakładce provisioning ustalamy przypisywanie punktom dostępu konfiguracji. W Hw. Supported Modes wybieramy najpierw gn (będzie to odpowiadało pasmu 2.4 GHz), Action: create dynamic enabled, Master Configuration: Nauczyciele 2.4, Slave Configuration: Uczniowie 2.4.



New CAPs Provisioning

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

Hw. Supported Modes: gn

Identity Regexp:

Common Name Regexp:

IP Address Ranges:

Action: create dynamic enabled

Master Configuration: Nauczyciele 2.4

Slave Configuration: Uczniowie 2.4

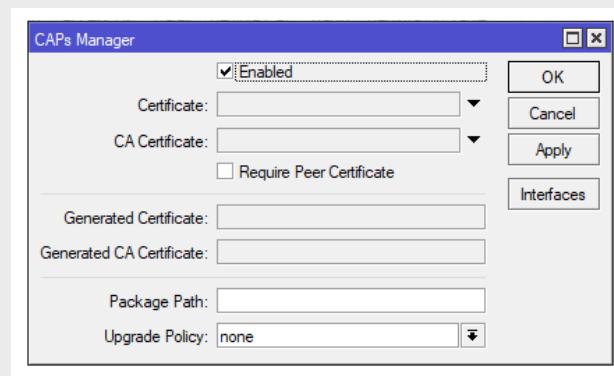
Name Format: cap

Name Prefix:

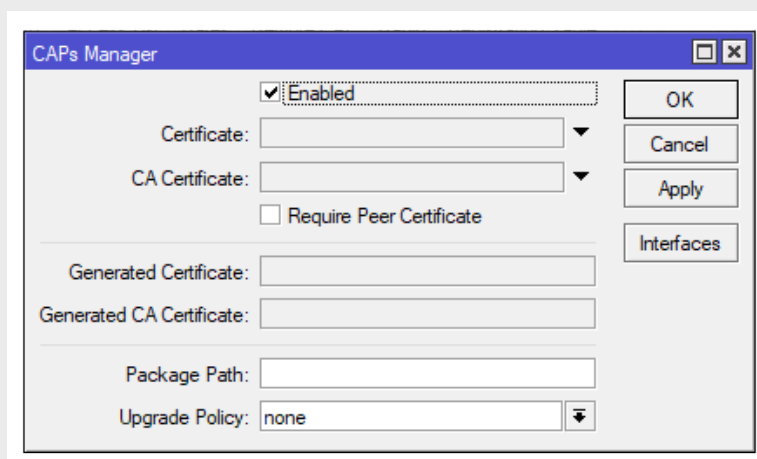
enabled

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

Podobnie ustalamy przypisywanie dla 5 GHz (Hw. Supported Modes: ac), konfiguracje wybieramy adekwatnie dla 5 GHz.



Teraz przechodzimy do uruchomienia CAPsMAN Manager'a, w tym celu otwieramy zakładkę CAP Interface, klikamy Manager, zaznaczamy Enabled i zatwierdzamy. Po chwili nasz router powinien połączyć się ze znalezionymi punktami dostępu i automatycznie je skonfigurować.



Źródła

<http://www.mwrf.com/active-components/what-s-difference-between-ieee-80211af-and-80211ah>



OGÓLNOPOLSKA
SIEĆ EDUKACYJNA

T: +48 22 182 55 55

E: ose@nask.pl

A: ul. Kolska 12

01-045 Warszawa

W: ose.gov.pl

NIP 5210417157

REGON 010464542



Ministerstwo
Cyfryzacji



MINISTERSTWO
EDUKACJI
NARODOWEJ

NASK