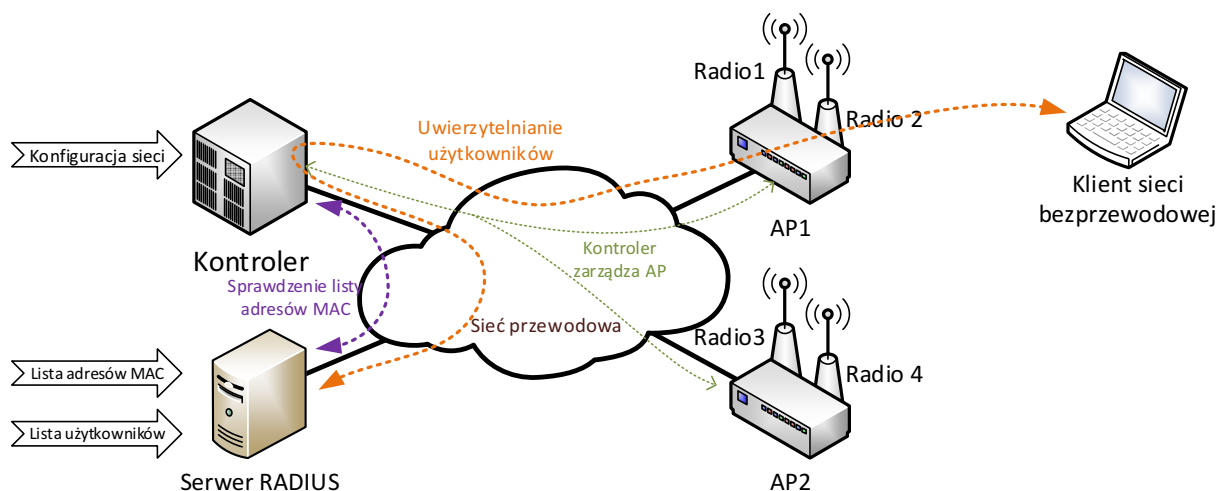


Wykorzystanie kontrolera sieci bezprzewodowej oraz serwera RADIUS

Kontroler sieci bezprzewodowej (Wireless Network Controller – WNC) może wykorzystywać wiele powiązanych z nim punktów dostępowych (Access Point – AP), z których każdy może posiadać wiele niezależnych interfejsów radiowych. AP nie są w stanie funkcjonować samodzielnie, a jedynie zarządzane przez kontroler (na rys. poniżej kolor zielony) – także ich konfiguracja odbywa się jedynie za pośrednictwem kontrolera.



Serwer RADIUS jest podczas laboratorium wykorzystywany na 2 sposoby: jako baza adresów MAC urządzeń dopuszczonych do pracy w sieci oraz w celu uwierzytelniania użytkowników i określenia czy mogą korzystać z sieci.

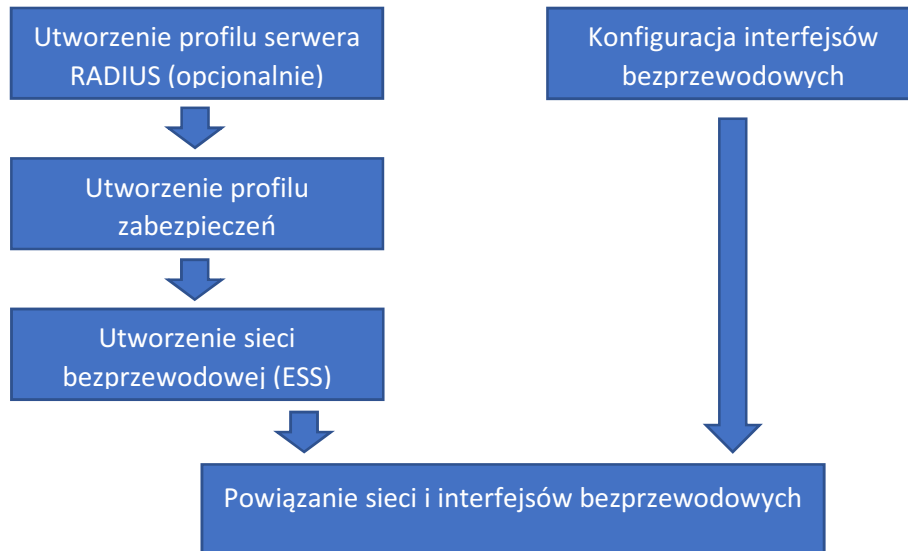
Przy przypadku wykorzystania serwera RADIUS jako bazy danych zawierającej adresy MAC, kontroler jest informowany przez AP o próbie dostępu podjętej przez urządzenie klienckie o określonym adresie MAC. Kontroler wysyła następnie zapytanie do dotyczące danego adresu MAC do serwera RADIUS, który określa czy kontroler powinien obsługiwać czy zignorować danego klienta i odsyła do kontrolera stosowaną informację.

Przy przypadku wykorzystania serwera RADIUS do uwierzytelniania użytkowników, serwer RADIUS przechowuje w swojej bazie danych informacje o kontach użytkowników (w przypadku tego laboratorium – nazw użytkowników i ich hasła). Klient sieci bezprzewodowej podłącza się do niej za pośrednictwem AP, lecz zanim nie przeprowadzi uwierzytelnienia, może komunikować się jedynie z serwerem RADIUS (co odbywa się za pośrednictwem AP i kontrolera – na rys. powyżej zaznaczono to kolorem pomarańczowym). Po udanym uwierzytelnieniu zarówno kontroler jak i klient sieci są informowani o powodzeniu tego procesu – od tego momentu klient jest w stanie korzystać z sieci bezprzewodowej. Jeśli bezprzewodowa sieć jest zabezpieczona mechanizmami WEP/WPA/WPA2 to serwer RADIUS może automatycznie wygenerować oraz przekazać kontrolerowi oraz klientowi klucz służący do zabezpieczenia komunikacji bezprzewodowej. Jest to jednak możliwe tylko w przypadku użycia niektórych protokołów uwierzytelniania.

Konfiguracja kontrolera sieci bezprzewodowej Fortinet MC3200-V

Instrukcja zawiera podstawowe informacje pozwalające na utworzenie sieci bezprzewodowej w środowisku systemu wykorzystującego kontroler sieci bezprzewodowej Fortinet MC3200-V.

Niezbędne kroki konfiguracji oraz ich właściwą kolejność przedstawia rysunek poniżej.



Zachowanie powyższej kolejności jest konieczne ze względu na fakt, iż wymienione elementy są wzajemnie powiązane i np. utworzenie sieci bezprzewodowej wymaga podania zdefiniowanego już wcześniej profilu zabezpieczeń. Sposób realizacji poszczególnych kroków konfiguracji przedstawiono w kolejnych rozdziałach.

1 Utworzenie profilu serwera RADIUS

Configuration -> Security -> RADIUS

Strona zawiera listę serwerów RADIUS z którymi współpracować ma dany kontroler (profile serwerów RADIUS) wraz z ich najważniejszymi parametrami. Ikona ołówka w pierwszej kolumnie tabeli pozwala na edycję istniejącego profilu, podczas gdy przyciski powyżej tabeli umożliwiają dodawanie nowych oraz prowadzenie operacji na grupie pozycji tabeli.

	RADIUS Profile Name	RADIUS IP	RADIUS Port	Remote RADIUS Server	RADIUS Relay AP-ID	MAC Address Delimiter	Password Type	Called-Station-ID Type	Owner	RADIUS Server Timeout	RADIUS Server Retries
	komp2	10.10.1.2	1812	Off	0	Colon ()	Shared Key	Default	controller	2	3

Dodanie nowego wpisu (przycisk **Add**) lub edycja istniejącego (ikona ołówka przy konkretnym wpisie) powoduje wyświetlenie strony pozwalającej na zdefiniowanie parametrów koniecznych do współpracy kontrolera z danym serwerem RADIUS. Wymagane pola zaznaczono gwiazdkami.

RADIUS Profiles - Add ?

RADIUS Profile Name *	<input type="text"/>	Enter 1-16 chars.
Description	<input type="text"/>	Enter 0-128 chars.
RADIUS IP *	<input type="text"/>	
RADIUS Secret *	<input type="text"/>	Enter 1- 64 chars.
RADIUS Port	<input type="text" value="1812"/>	Valid range: [1024-65535]
Remote RADIUS Server	<input type="checkbox"/>	
RADIUS Relay AP-ID	No Data for RADIUS Relay AP-ID	
MAC Address Delimiter	<input type="text" value="Hyphen (-)"/>	
Password Type	<input type="text" value="Shared Key"/>	
Called-Station-ID Type	<input type="text" value="Default"/>	
COA	<input type="checkbox"/>	
RADIUS Server Timeout	<input type="text" value="2"/>	Valid range: [1-20]
RADIUS Server Retries	<input type="text" value="3"/>	Valid range: [1-10]

Najważniejsze pola to:

- **RADIUS Profile Name** – nazwa danego profilu, używana do wybrania danego serwera RADIUS
- **RADIUS IP** – adres IP serwera,
- **RADIUS Secret** – hasło wykorzystywane do ochrony komunikacji pomiędzy serwerem RADIUS i kontrolerem. Powinno być zgodne z hasłem zdefiniowanym dla danego kontrolera w pliku clients.conf serwera RADIUS.

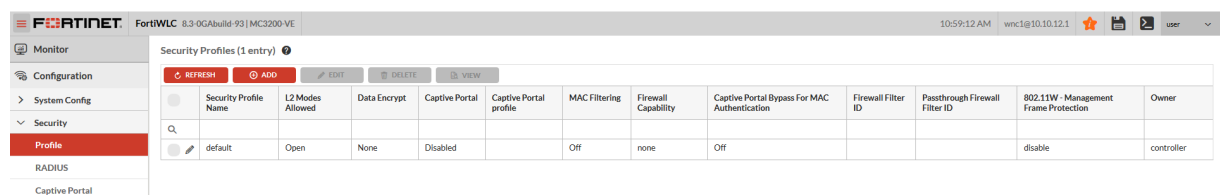
Pola mające istotne znaczenie przy wykorzystaniu serwera RADIUS jako bazy adresów MAC dla potrzeb realizacji filtracji klientów wg powyższych adresów:

- **MAC Address Delimiter** – znak rozdzielający bajty adresu MAC w zapytaniu przesyłanym przez kontroler do serwera,
- **Password Type** – określa zawartość pola Password w zapytaniu o dopuszczenie danego adresu MAC, przesyłanego przez kontroler do serwera.

2 Utworzenie profilu zabezpieczeń

Configuration -> Security -> Profile

Strona zawiera listę tzw. profili zabezpieczeń, czyli definicji mechanizmów bezpieczeństwa wykorzystywanych następnie w utworzonych sieciach bezprzewodowych. Dostępne przyciski oraz sposób edycji wpisów jest analogiczny jak w przypadku opisanej wcześniej listy serwerów RADIUS.



Security Profile Name	L2 Modes Allowed	Data Encrypt	Captive Portal	Captive Portal profile	MAC Filtering	Firewall Capability	Captive Portal Bypass For MAC Authentication	Firewall Filter ID	Passthrough Firewall Filter ID	802.11W - Management Frame Protection	Owner
default	Open	None	Disabled		Off	none	Off			disable	controller

Po utworzeniu lub rozpoczęciu edycji nowego profilu bezpieczeństwa, pojawia się strona pozwalająca na określenie jego parametrów, podzielona na kilka sekcji. Wymagane pola zaznaczono gwiazdkami.

Security Profiles - Add ?

Security Profile Name *	<input type="text"/>	Enter 1-32 chars.
SECURITY SETTINGS		
Security Mode *	Open	▼
CAPTIVE PORTAL SETTINGS		
Captive Portal	Disabled	▼
Passthrough Firewall Filter ID	<input type="text"/>	Enter 0-16 chars.
MAC FILTERING SETTINGS		
MAC Filtering	Off	▼
FIREWALL SETTINGS		
Firewall Capability	none	▼
GENERAL SETTINGS		
Security Logging	Off	▼

W naszym przypadku wykorzystywane będą:

- Pole **Security Profile Name** – nazwa profilu pozwalająca na jego powiązanie z tworzoną siecią bezprzewodową.
- Sekcja **Security Settings** – zawierająca ustawienia bezpośrednio związane uwierzytelnianiem klientów oraz ochroną ruchu sieciowego,
- Sekcja **MAC Filtering Settings** – umożliwia skonfigurowanie filtrów adresów MAC.

2.1 Security Profile - Security Settings

Sposób uwierzytelniania klienta oraz ochrony ruchu sieciowego określany jest przez wybór odpowiedniej wartości pola **Security Mode**, co powoduje pojawienie się dalszych opcji konfiguracyjnych, specyficznych dla wybranego mechanizmu zabezpieczeń.

- **Open** – sieć bez uwierzytelniania (uwierzytelnianie otwarte) oraz bez ochrony przesyłanego ruchu,
- **Enterprise** – grupa mechanizmów wymagających serwera RADIUS, którego profil powinien być zdefiniowany z użyciem opisanej wcześniej strony Configuration -> Security -> RADIUS. W przypadku każdego z nich należy wskazać odpowiedni profil serwera RADIUS w polu **Primary RADIUS Profile Name**.

OPCJA TUNNEL TERMINATION POWINNA BYĆ WYŁĄCZONA.

- 802.1x/Open – sieć wymagająca uwierzytelniania 802.1x, bez ochrony ruchu sieciowego,
- 802.1x/WEPxx – sieć wymagająca uwierzytelniania 802.1x, wykorzystująca do ochrony ruchu sieciowego mechanizm WEP z kluczem 64 lub 128 bitowym,

- WPA2/CCMP-AES, WPA2/CCMP-TKIP – sieć wymagająca uwierzytelniania 802.1x, wykorzystująca do ochrony ruchu sieciowego mechanizm WPA2 oraz algorytmy kryptograficzne odpowiednio AES lub TKIP.
- Mixed/CCMP-TKIP – sieć wymagająca uwierzytelniania 802.1x, wykorzystująca do ochrony ruchu sieciowego mechanizm WPA lub WPA2 oraz algorytmy kryptograficzne TKIP.
- **Personal** – grupa mechanizmów wykorzystujących w celu kontroli dostępu do sieci hasło wspólne dla wszystkich użytkowników.
 - **Static WEP/WEPxx** – sieć zabezpieczona z użyciem klasycznego mechanizmu WEP o długości klucza 64 lub 128 bitów,
 - Należy wypełnić pole **WEP Key (Alphanumeric/Hexadecimal)** – podajemy tu klucz WEP w postaci:
 - ciągu bajtów zapisanych heksadecymalnie poprzedzonego oznaczeniem 0x (np. 0x6427a49e31),
 - lub ciągu znaków ASCII.

Dla WEP64 klucz powinien być długości 5 bajtów, a dla WEP128 długości 13 bajtów.
 - Pole **Shared Key Authentication** pozwala uruchomić mechanizm uwierzytelniania WEP Shared Key (On). Jeśli będzie on wyłączony (Off) wykorzystywane będzie uwierzytelniania WEP Open System.
 - **WPA2/CCMP-AES, WPA2/CCMP-TKIP** – wykorzystująca do ochrony ruchu sieciowego mechanizm WPA2 oraz algorytmy kryptograficzne odpowiednio AES lub TKIP,
 - Należy wypełnić pole **Pre-shared Key (Alphanumeric/Hexadecimal)** podając hasło WPA w postaci:
 - ciągu znaków ASCII od długości 8-63 znaków,
 - ciągu bajtów zapisanych heksadecymalnie poprzedzonego oznaczeniem 0x (np. 0x6427a49e31) o długości 8-64 bajtów.
 - **Mixed/CCMP-TKIP** – sieć wykorzystująca do ochrony ruchu sieciowego mechanizm WPA lub WPA2 oraz algorytmy kryptograficzne TKIP. Podobnie jak w przypadku WPA2 należy wypełnić pole **Pre-shared Key (Alphanumeric/Hexadecimal)**.

2.2 Security Profile - MAC Filtering Settings

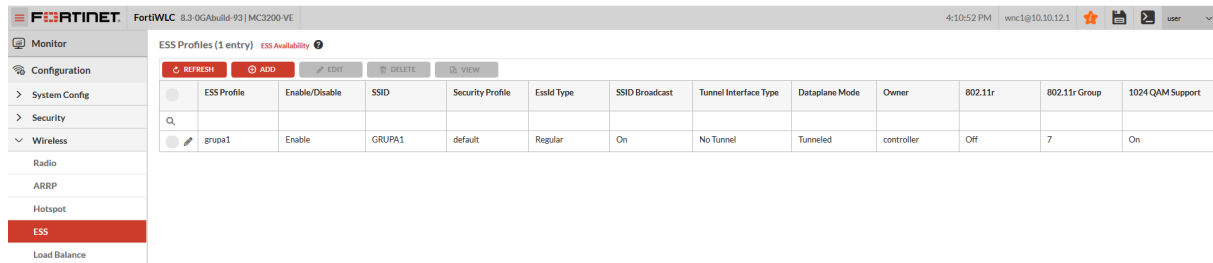
Pole **MAC Filtering** pozwala włączyć (On) lub wyłączyć (Off) funkcje filtrowania odbieranych ramek bezprzewodowych na podstawie adresów MAC klientów. Po włączeniu powyższej funkcjonalności pojawiają się dalsze pola konfiguracyjne:

- **ACL Environment State** – umożliwia podjęcie decyzji czy funkcja filtracji ma decydować o dopuszczeniu lub odrzuceniu klienta, czy jedynie służyć rozliczaniu (accounting).
 - Disabled – brak filtrowania (wszystkie stacje są dopuszczane),
 - Permit List Enabled – adresy nieobecne w bazie są domyślnie odrzucane,
 - Deny List Enabled – adresy nieobecne w bazie są domyślnie dopuszczane.
- **MAC Auth Primary RADIUS Profile Name** – pozwala wybrać profil serwera RADIUS, który ma być wykorzystywany do określenia, czy dany adres MAC ma być dopuszczony czy odrzucony.

3 Utworzenie sieci bezprzewodowej

Configuration -> Wireless -> ESS

Strona zawiera listę utworzonych sieci bezprzewodowych. Sposób edycji wpisów jest analogiczny jak w przypadku list opisanych wcześniej.

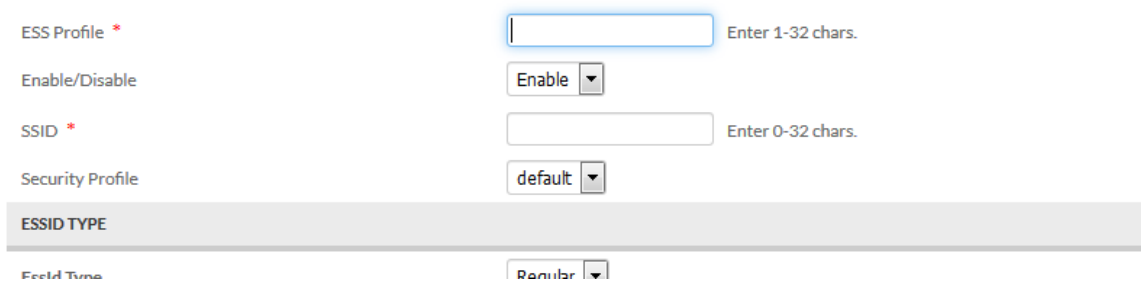


The screenshot shows the FortiNet FortiWLC configuration interface. The left sidebar contains a navigation menu with options like Monitor, Configuration, System Config, Security, Wireless, Radio, ARRP, Hotspot, ESS, and Load Balance. The main content area displays 'ESS Profiles (1 entry)' with a table of configurations. The table has columns for ESS Profile, Enable/Disable, SSID, Security Profile, Essk Type, SSID Broadcast, Tunnel Interface Type, Dataplane Mode, Owner, 802.11r, 802.11r Group, and 1024 QAM Support. One entry is visible with the name 'grupa1'.

ESS Profile	Enable/Disable	SSID	Security Profile	Essk Type	SSID Broadcast	Tunnel Interface Type	Dataplane Mode	Owner	802.11r	802.11r Group	1024 QAM Support
grupa1	Enable	GRUPA1	default	Regular	On	No Tunnel	Tunneled	controller	Off	7	On

Po utworzeniu lub rozpoczęciu edycji nowej sieci bezprzewodowej, pojawia się strona pozwalająca na określenie jej parametrów, podzielona na kilka sekcji. Wymagane pola zaznaczono gwiazdkami.

ESS Profiles - Add ?



The screenshot shows the 'ESS Profiles - Add' configuration form. It includes several input fields and dropdown menus:

- ESS Profile ***: A text input field with a placeholder 'Enter 1-32 chars.'
- Enable/Disable**: A dropdown menu with 'Enable' selected.
- SSID ***: A text input field with a placeholder 'Enter 0-32 chars.'
- Security Profile**: A dropdown menu with 'default' selected.
- ESSID TYPE**: A dropdown menu with 'Regular' selected.

Interesujące nas pola to:

- **ESS Profile** – wewnętrzna nazwa utworzonej sieci, pod którą będzie widoczna na liście sieci obsługiwanych przez kontroler. NIE jest to nazwa sieci widziana przez podłączających się klientów.
- **Enable/Disable** – włączenie (Enable) lub wyłączenie (Disable) danej sieci bezprzewodowej.
- **SSID** – nazwa sieci bezprzewodowej pod którą będzie widziana przez podłączających się użytkowników.
- **Security Profile** – umożliwia wybór zdefiniowanego wcześniej profilu zabezpieczeń, który ma być wykorzystywany w danej sieci.

NALEŻY WYŁĄCZYĆ OPCJĘ „IP Prefix Validation” W SEKCJI „DATAPLANE MODE”.

3.1 Powiązanie sieci bezprzewodowej z interfejsami radiowymi

Jeśli pole **New AP's Join ESS** w sekcji **General Settings** jest ustawione na **On**, to nowo utworzona sieć zostanie uruchomiona na wszystkich dostępnych dla danego kontrolera interfejsach bezprzewodowych kontrolowanych przez niego punktów dostępowych. Jeśli pole to jest ustawione na **Off**, to sieć będzie musiała zostać ręcznie powiązana z interfejsami radiowymi punktów dostępowych które mają ją udostępniać.

Aby powiązać sieć bezprzewodową z określonymi interfejsami radiowymi, należy zatwierdzić jej utworzenie wybierając przycisk **Save**, po czym ponownie rozpocząć edycję jej parametrów wybierając ikonę ołówka w pierwszej kolumnie listy utworzonych sieci. Po wczytaniu strony pozwalającej na edycję parametrów sieci, z listy zakładek widocznej w jej górnej części wybieramy **ESS-AP Table**.

ESS-AP Configuration (2 entries) ?

ESS Profile | **ESS-AP Table** | Security Profiles | Hotspot Profiles

REFRESH | ADD | EDIT | DELETE | VIEW

	ESS Profile	AP ID	AP Name	Interface Index	Channel	Operating Channel	Admin State	Max Calls	BSSID	Owner
<input type="checkbox"/>	grupa1	1	AP-1	2	36	36	Up	0	00:0c:e6:0a:0b:46	controller
<input type="checkbox"/>	grupa1	1	AP-1	1	6	6	Up	0	00:0c:e6:0a:db:f9	controller

Zakładka **ESS-AP Table** zawiera listę interfejsów radiowych z którymi dana sieć bezprzewodowa jest w tej chwili powiązana (tzn. oferują one dostęp do danej sieci bezprzewodowej).

Usunięcie interfejsów z powyższej listy wymaga zaznaczenia szarego pola wyboru widocznego w pierwszej kolumnie odpowiadających im wierszy tabeli i użycie przycisku **Delete** umieszczonego powyżej.

Dodanie nowego interfejsu do listy możliwe jest z użyciem przycisku **Add**, co spowoduje pojawienie się listy interfejsów radiowych z którym dana sieć nie jest jeszcze powiązana. W celu dodania interfejsów do listy oferujących dostęp do danej sieci, zaznaczamy szare pole wyboru w pierwszej kolumnie odpowiednich wpisów i naciskamy przycisk **Save** widoczny w prawym dolnym rogu strony.

4 Ustawienia interfejsów bezprzewodowych

Configuration -> Wireless -> Radio

Strona zawiera listę wszystkich interfejsów bezprzewodowych dostępnych dla kontrolera. Interfejsy te zainstalowane są w punktach dostępowych (Access Point – AP) powiązanych z danym kontrolerem.

Kolumny **AP ID** oraz **AP Name** wskazują punkt dostępowy (odpowiednio jego numer kolejny oraz nazwę), podczas gdy kolumna **Interface Index** określa numer interfejsu bezprzewodowego w obrębie danego AP. W przykładowej konfiguracji widocznej na ilustracji poniżej, kontroler współpracuje z pojedynczym punktem dostępowym (AP-1) wyposażonym w 2 interfejsy bezprzewodowe.

Fortinet FortiWLC 4.3-0GAbuild-93 | MC3200-VE | 7:11:10 PM | wnc1@10.10.12.1 | user

Monitor | Wireless Interface Configuration (2 entries) ?

REFRESH | EDIT | BULKUPDATE | VIEW

	AP ID	AP Name	Interface Index	AP Model	Administrative Status	Operational Status	Primary Channel	Operating Channel	RF Band Selection	VHT Service Status	AP Mode	Channel Width	Mesh Service Admin Status	Uplink Type	Feature Group Name	Override Group Settings
<input type="checkbox"/>	1	AP-1	2	AP832e	Up	Disabled	36	36	802.11ac	Disable	Service Mode	80 MHz	Disable	Downlink	-	Off
<input type="checkbox"/>	1	AP-1	1	AP832e	Up	Disabled	6	6	802.11bgn	Disable	Service Mode	20 MHz	Disable	Downlink	-	Off

Edycja parametrów interfejsów możliwa jest po wybraniu ikony ołówka widocznej w pierwszej kolumnie każdego wiersza tabeli. Po jej wybraniu pojawia się strona pozwalająca na modyfikację parametrów konkretnego interfejsu bezprzewodowego.

Wireless Interface Configuration - Update

Wireless Interface

Wireless Statistics

Antenna Property

AP ID	1
IfIndex	1
AP Model	AP832e

Interface Description	<input type="text" value="ieee80211-1-1"/> <small>Enter 0-256 chars.</small>
Administrative Status	<input type="button" value="Up"/>
Primary Channel	<input type="button" value="6"/>
Short Preamble	<input type="button" value="On"/>
RF Band Selection	<input type="button" value="802.11bgn"/>
Transmit Power(EIRP)	<input type="text" value="20"/>
AP Mode	<input type="button" value="Service Mode"/>
B/G Protection Mode	<input type="button" value="Auto"/>
HT Protection Mode	<input type="button" value="Off"/>
Channel Width	<input type="button" value="20 MHz"/>
MIMO Mode	<input type="button" value="3x3"/>
802.11n only mode	<input type="button" value="Off"/>
Probe Response Threshold	<input type="text" value="15"/> <small>Valid range: [0-100]</small>
Mesh Service Admin Status	<input type="button" value="Disable"/>
Transmit Beamforming Support	<input type="button" value="Disabled"/>
STBC Support	<input type="button" value="Off"/>
DFS Fallback Option	<input type="button" value="Disable"/>
DFS Fallback Channel	<input type="button" value="6"/>
DFS Channel Revertive(minutes)	<input type="text" value="30"/> <small>Valid range: [30-1440]</small>

[Show Detail Info...](#)

W górnej części strony widoczne są 3 zakładki, z których interesuje nas domyślnie wybrana: **Wireless Interface**. Z widocznych na niej parametrów, konfigurujemy:

- **Administrative Status** – umożliwia włączenie (**UP**) lub wyłączenie (**DOWN**) interfejsu bezprzewodowego.
- **Primary Channel** – kanał pracy interfejsu. Lista możliwych do wyboru wartości zależy od ustawienia pola RF Band Selection.
- **RF Band Selection** – pozwala na wybór standardu komunikacji obsługiwanej przez interfejs, a jednocześnie pasma w którym będzie on pracował:
 - 802.11b, 802.11g, 802.11bg, 802.11bgn – pasmo 2.4 GHz (dostępne kanały 1-13),
 - 802.11a, 802.11an, 802.11ac – pasmo 5 GHz (dostępne kanały 36-140).
- **AP Mode** – pozwala na wskazanie trybu pracy interfejsu. Aby mógł on obsługiwać podłączających się do sieci klientów, pole to musi być ustawione na wartość **Service Mode**.
- **Channel Width** – w przypadku standardów umożliwiających pracę z różną szerokością kanału częstotliwościowego, pole to pozwala na wybór jego szerokości. O ile w zadaniu nie nakazano inaczej, należy zastosować wartość **20 MHz**.