SIECI BEZPRZEWODOWE WYKORZYSTUJĄCE TECHNOLOGIE WIRTUALNEJ KOMÓRKI I WIRTUALNEGO PORTU NA PRZYKŁADZIE MERU NETWORKS

Mariusz Piwiński[1], *Grzegorz Marczak*[2]
[1] *Instytut Fizyki, Wydział Fizyki, Astronomii i Informatyki Stosowanej*
Uniwersytet Mikołaja Kopernika
ul. Grudziądzka 5
87-100 Toruń
Mariusz.Piwinski@fizyka.umk.pl

[2] *Wydział Matematyki i Informatyki*
Uniwersytet Mikołaja Kopernika
ul. Chopina 12/18
87-100 Toruń
lielow@mat.umk.pl

Abstract: In this paper the main aspects of using wireless networks (IEEE 802.11 standards) will be presented. The authors will try to answer the question: What is the main advantage of using wireless controller with virtual cell and virtual port technologies.

1. Wstęp

Obecnie mamy do czynienia z bardzo dynamicznym rozwojem sieci bezprzewodowych wykorzystujących różne technologie. Jedną z nich jest Wi-Fi, którą definiuje standard IEEE 802.11 z wszystkimi swoimi rozszerzeniami [4]. Jednocześnie lawinowy wzrost liczby urządzeń korzystających z tego rozwiązania spowodował, iż coraz częściej widoczne są ograniczenia stosowanych technologii dostępowych. Sytuację pogarsza fakt wykorzystywania przez sieci Wi-Fi częstotliwości nielicencjonowanych, co oznacza, iż mogą być one używane również przez inne

urządzenia takie jak układy zdalnego sterowania, nianie automatyczne, urządzenia Bluetooth, a nawet zdalnie sterowane modele. Wszystkie te urządzenia wpływają na znaczne zaszumienie dostępnego pasma, co ostatecznie przyczynia się do pogorszenia jakości transmisji przesyłanych danych pomiędzy urządzeniami mobilnymi. Sytuację często dodatkowo komplikuje wielkość oraz złożoność obszaru, na którym ma być dostępna sieć bezprzewodowa. Ze względu na ograniczenia technologiczne rozległe sieci muszą być budowane z zastosowaniem dużej liczby punktów dostępowych. Urządzenia te wymagają odpowiedniej, często nietrywialnej konfiguracji, co w znaczący sposób utrudnia administrowanie taką siecią. W przypadku stosowania większej ilości punktów dostępowych, zarządzanie siecią bezprzewodową poprzez indywidualną konfigurację poszczególnych urządzeń staje się bardzo trudne, a czasami wręcz niemożliwe do wykonania. W związku z powyższym w takich sytuacjach coraz częściej stosowanym rozwiązaniem jest zarządzanie globalne wykorzystujące różnego rodzaju kontrolery. Niestety pomimo takiego podejścia trudno jest uniknąć problemów związanych z zakłóceniami oraz ograniczoną liczbą dostępnych kanałów, które mogą być wykorzystywane przez stosowane technologie. W efekcie może prowadzić to do znacznego ograniczenia możliwości wykorzystania sieci oraz zmniejszenia pasma dostępnego dla podłączonego użytkownika.

Jednym z rozwiązań, które pozwala na uniknięcie części z tych problemów jest technologia wirtualnej komórki oraz wirtualnego portu realizowana w sieciach Meru Networks. Celem niniejszego opracowania jest przedstawienie podstawowych aspektów związanych z zarządzaniem siecią bezprzewodową w oparciu o kontroler oraz wskazanie zalet związanych ze stosowaniem takiego podejścia.

Opisywane rozwiązania dotyczące sieci bezprzewodowych zostały wybrane przez Cyfrową Szkołę, jako najlepsze rozwiązanie sprawdzone w edukacji. Więcej informacji można znaleźć pod adresem http://fen.pl/cyfrowaszkola/ [3].

2. Podstawowe pojęcia

W celu prawidłowego zrozumienia sposobu działania sieci bezprzewodowych niezbędne jest wprowadzenie podstawowych pojęć, które będą wykorzystywane w niniejszym opracowaniu.

- **AP** – (*ang. access point*) urządzenie zapewniające urządzeniom klienckim dostęp do sieci komputerowej za pomocą medium radiowego.
- **BSS** – (*ang. Basic Service Set*) według standardu IEEE 802.11 jest to grupa logicznie powiązanych ze sobą urządzeń bezprzewodowych. BSS stanowi podstawową komórkę sieci bezprzewodowej, która składa się z przy-

najmniej jednego punktu dostępowego (AP) oraz urządzenia klienckiego (STA).

- **BSSID** – (*ang. Basic Service Set Identifier*) 48-bitowy numer identyfikacyjny w sieciach bezprzewodowych standardu IEEE 802.11 nadawany punktom dostępowym, umożliwiający jednoznaczną identyfikację podstawowej komórki sieci bezprzewodowej (BSS). Jest on odpowiednikiem adresu MAC dla technologii Ethernet.
- **DSSS** – (*ang. Direct Sequence Spread Spectrum*) technika rozpraszania widma w systemach szerokopasmowych przy pomocy ciągów kodowych.
- **EAP** – (*ang. Extensible Authentication Protocol*) framework autentykacyjny, pozwalający na wykorzystanie różnych algorytmów uwierzytelnienia w ujednolicony sposób.
- **ESS** – (*ang. Extended Service Set*) rozszerzona komórka sieci bezprzewodowej składająca się z dwóch lub więcej komórek podstawowych (BSS), wykorzystująca tą samą nazwę sieci SSID, która w tym przypadku nazywana jest identyfikatorem rozszerzonej komórki (ESSID)
- **FHSS** – (*ang. Frequency-hopping spread spectrum*) metoda rozpraszania widma w systemach szerokopasmowych, polegająca na skokowych zmianach częstotliwości sygnału co określoną jednostkę czasu w obrębie kanału.
- **IEEE 802.11** – grupa standardów IEEE opisujących warstwę fizyczną i podwarstwę MAC (warstwa 2 Modelu OSI) bezprzewodowych sieci lokalnych.
- **Interferencja** – zjawisko powstawania nowego, przestrzennego rozkładu amplitudy fali (wzmocnienia i wygaszenia) w wyniku nakładania się dwóch lub więcej fal.
- **OFDM** – (ang. *Orthogonal Frequency-Division Multiplexing*) metoda kodowania danych cyfrowych w oparciu o częstotliwości podnośne.
- **SSID** – (ang. *Service Set Identifier)* identyfikator sieci o długości do 32 znaków, dodawany do nagłówków pakietów wysyłanych przez bezprzewodową sieć lokalną. Jest to identyfikator umożliwiający klientowi rozpoznanie rozgłaszanej sieci.
- **STA** – (ang. *Station)* urządzenie posiadające możliwość korzystania z sieci bezprzewodowej, tzw. klient bezprzewodowy.
- **STAID**– (*ang. Station Identifier*) 48-bitowy numer identyfikacyjny w sieciach bezprzewodowych standardu IEEE 802.11 nadawany interfejsom ra-

diowym stacji klienckich, umożliwiający ich jednoznaczną identyfikację Jest on odpowiednikiem adresu MAC dla technologii Ethernet.

- **TKIP** – (ang. *Temporal Key Integrity Protocol*) wykorzystujący RC4 protokół używany w celu zabezpieczenia warstwy łącza danych w sieciach bezprzewodowych zgodnych ze standardem IEEE 802.11. Obecnie nie zalecany do stosowania.
- **WEP** – (ang. *Wired Equivalent Privacy*) standard szyfrowania w sieciach bezprzewodowych, oparty na algorytmie RC4, z powodu powszechnie dostępnych algorytmów i programów umożliwiających jego uzyskanie z obserwowanych ramek obecnie nie zalecany do stosowania.
- **WPA** – (ang. *Wi-Fi Protected Access*) standard szyfrowania w sieciach bezprzewodowych, oparty o 802.1x, EAP, TKIP i MIC. Występuje w wersji personal (hasło współdzielone) i enterprise (współpraca z serwerem Radius). Obecnie nie zalecany do stosowania.
- **WPA2** – **(**ang. *Wi-Fi Protected access II*) następca WPA, wykorzystujący algorytm AES zamiast RC4. Podobnie jak WPA posiada wariant personal i enterprise.

3. Technologie Wi-Fi

Współistnienie wielu różnych ogólnie dostępnych technologii bezprzewodowych umożliwiających transmisję danych (Wi-Fi IEEE 802.11 [6], Bluetooth [2], WiMAX IEEE 802.16 [7]) powoduje, iż na rynku istnieje obecnie bardzo dużo wykorzystujących je urządzeń. Niestety ze względu na politykę producentów oraz początkowy brak systemu zewnętrznej certyfikacji produktów zdarzało się, że urządzenia różnych firm pomimo, iż stosowały teoretycznie ten sam standard komunikacji nie mogły się ze sobą poprawnie komunikować. Obecnie istnieje kilka organizacji oraz konsorcjów zajmujących się określaniem standardów komunikacji oraz certyfikacją produkowanych urządzeń, ich nazwy oraz znaki logo przedstawiono na Rysunku 1. W przypadku urządzeń bezprzewodowych działających w standardzie 802.11 organizacją zajmującą się certyfikacją jest Wi-Fi Alliance. Po pomyślnym przeprowadzeniu serii testów konkretne urządzenie może otrzymać jedną z dostępnych etykiet, potwierdzającą zgodność z testowanymi standardami (Rysunek 2). Ponadto konsorcjum to prowadzi na swojej stronie WWW bazę danych zawierającą informacje o wszystkich certyfikowanych produktach, co pozwala na szybką weryfikację zgodności urządzenia sieciowego z konkretnym standardem [6].

Rysunek 1. Organizacje zajmujące się standaryzacją technologii transmisji danych

Rysunek 2. Etykiety certyfikacyjne przydzielane przez Wi-Fi Alliance.[6]

Różne typy certyfikatów związane są z różnymi rozszerzeniami standardu IEEE 802.11, który na przestrzeni lat ewoluował zapewniając użytkownikom coraz większe prędkości przesyłania danych. Ze względu na fakt, iż nadal mogą istnieć użytkownicy wykorzystujący stare karty bezprzewodowe, producenci nowych urządzeń starają się zadbać o ich wsteczną kompatybilność, tak aby mogły równocześnie komunikować się z klientami pracującymi w różnych standardach. Jednakże ze

względu na optymalizację pasma w sieci bezprzewodowej obecnie konfiguracje takie nie są zalecane.

Tabela 1. Standardy IEEE 802.11

Nazwa	Szybkości (Mb/s)	Pasmo (GHz)	Typ modulacji
802.11	1, 2	2,4	FHSS, DSSS, IR
802.11a	6, 9, 12, 18, 24, 36, 48, 54	5	OFDM
802.11b	1, 2, 5.5, 11	2,4	HR-DSSS,CCK
802.11g	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54	2,4	HR-DSSS, CCK, OFDM
802.11n	100, 150, 300, 450, 600	2,4 lub 5	OFDM
802.11ac	433, 867, 1300, 1733, ..., 6928	5	OFDM

Należy zwrócić uwagę, iż poszczególne standardy 802.11 wykorzystują różne nielicencjonowane pasma częstotliwości (2,4 GHz lub 5 GHz) oraz różne rodzaje modulacji związane ze sposobem przesyłania danych. Ich szczegółowy opis wykracza poza zakres tego opracowana.

Potrzeba zapewnienia dużej przepustowości łącza wymaga wykorzystania kanałów radiowych o jak największej szerokości. Dla standardów 802.11 b,g,n wykorzystywane jest nielicencjonowane (w większości krajów) pasmo 2,4 GHz, które na potrzeby Wi-Fi podzielono na kanały o szerokości wynoszącej 22 MHz (Tabela 2). W przypadku Polski (oraz większości Europy) regulacje prawne określają, iż nielicencjonowane pasmo może być wykorzystywane w zakresie częstotliwości od 2400,0 do 2483,5 MHz. Oznacza to, że w praktyce możemy wykorzystywać 13 dostępnych kanałów. W przypadku USA kanałów tych jest tylko 11, a w Japonii możliwe jest wykorzystanie również kanału nr 14. Regulacje prawne w precyzyjny sposób określają również maksymalną moc nadawania, która wynosi 100 mW.

Należy tutaj podkreślić, że punkt dostępowy dostosowany do norm europejskich, a uruchomiony w USA, może działać np. na kanale nr 13, ale będzie to w sprzeczności z obowiązującym w tym kraju prawem. Przewożenie punktów dostępowych do innych krajów i implementowanie ich w tamtejszych sieciach jest dosyć rzadką sytuacją. Należy jednakże zwrócić uwagę, iż podobne problemy związane z regulacjami prawnymi mogą pojawić się również w sytuacji gdy odwiedzający nas goście z USA będą próbowali podłączyć swoje urządzenia do naszej sieci bezprzewodowej pracującej na kanale nr 13. Może okazać się, że ich sprzęt nie pozwala na obsługę kanału wyższego niż kanał o numerze 11.

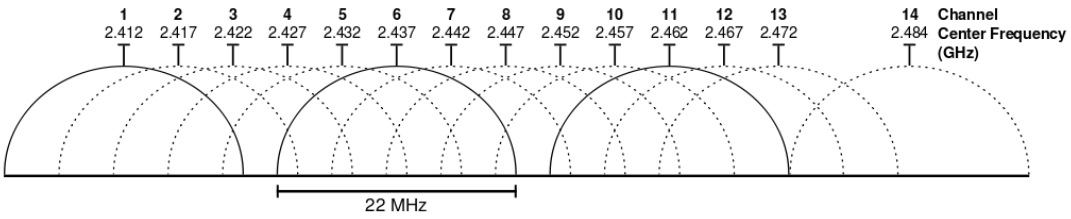
Dla uporządkowania informacji należy stwierdzić, iż pierwotny podział pasma 2,4 GHz na 22 MHz kanały został zrealizowany dla standardu 802.11 i jego rozszerzenia 802.11b. Nowsze standardy (802.11g,n) wykorzystują kanały 20 MHz, co jednakże nie wpływa w znaczący sposób na rozwiązanie opisywanych problemów.

Innym aspektem powiązanym z kanałami jest problem zakłóceń. Ze względu sposób działania urządzeń punkty dostępowe obsługujące różne sieci na tym samym obszarze powinny używać różnych kanałów, tak aby obsługiwane przez nie transmisje nie zakłócały się wzajemnie.

Tabela 2. Zakresy kanałów dla pasma 2,4 GHz, IEEE 802.11b.

Numer kanału	Dolna częstotliwość kanału [GHz]	Centralna częstotliwość kanału [GHz]	Górna częstotliwość kanału [GHz]
1	2,401	2,412	2,423
2	2,406	2,417	2,428
3	2,411	2,422	2,433
4	2,416	2,427	2,438
5	2,421	2,432	2,443
6	2,426	2,437	2,448
7	2,431	2,442	2,453
8	2,436	2,447	2,458
9	2,441	2,452	2,463
10	2,446	2,457	2,468
11	2,451	2,462	2,473
12	2,456	2,467	2,478
13	2,461	2,472	2,483
14	2,473	2,484	2,495

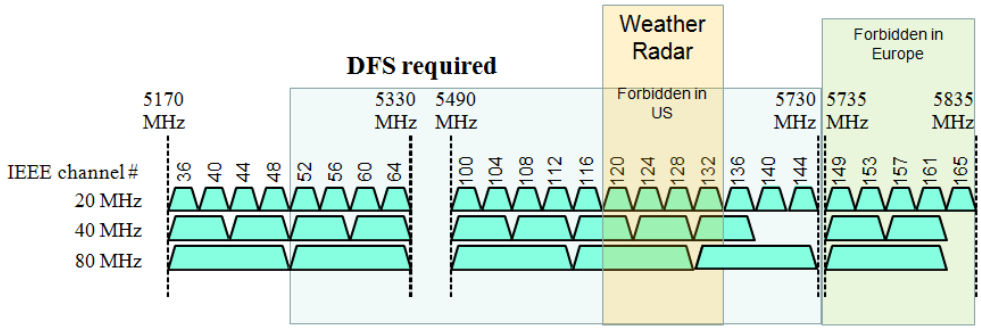
Niestety jak widać z zamieszczonej Tabeli 2, opisywane kanały nie są w pełni separowalne, a definiujące je częstotliwości centralne oddalone są od siebie tylko o 5 MHz, co stanowi około ¼ szerokości kanału. W praktyce oznacza, to że mamy do dyspozycji zaledwie trzy w pełni niezakłócające się kanały (np.1,7,13). Próba jednoczesnego użycia większej liczby kanałów przez różne urządzenia na tym samym obszarze, skutkować będzie wzajemnym zakłócaniem się i pogorszeniem parametrów transmisji. Problem ten został przedstawiony na Rysunku 3.



Rysunek 3. Graficzna reprezentacja przydziału kanałów dla standardu 802.11b dla pasma 2,4GHz (en.wikipedia.org/wiki/IEEE_802.11)

Wnikliwy czytelnik mógłby zadać sobie pytanie, dlaczego zatem dokonano takiego „dziwnego podziału" pasma. Odpowiedź związana jest z faktem, iż różne punkty dostępowe w praktyce nie są umieszczone w tym samym miejscu, wyposażone są w różne anteny, oddzielone różnymi ścianami o różnej tłumienności. Zatem podczas analizy zakłóceń należy przede wszystkim uwzględnić amplitudę sygnału, który dociera do nas z urządzenia obsługującego inną sieć. Ostatecznie oznacza to, że duża liczba kanałów umożliwia lepsze wykorzystanie dostępnego pasma przez wiele urządzeń.

Zgodnie z Tabelą 1 widać, iż standardy 802.11 a,n wykorzystują nielicencjonowane pasmo 5 GHz. W tym przypadku zostało one podzielone na niezachodzące się 20 MHz kanały, tak jak to przedstawiono na Rysunku 4.



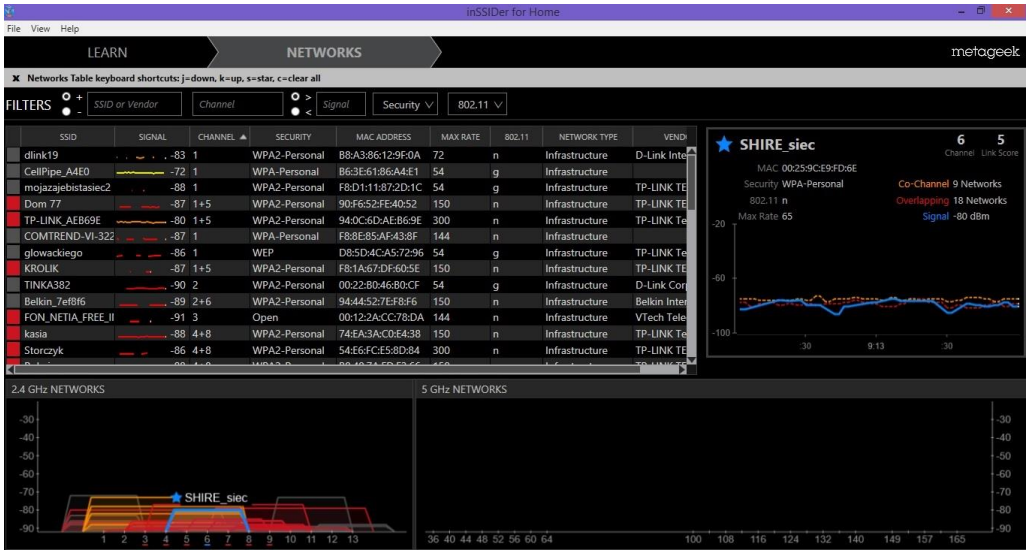
Rysunek 4. Organizacja pasma 5GHz (http://www.merunetworks.com).

Z pozoru sytuacja w paśmie 5 GHz jest lepsza, jednakże należy pamiętać, iż ze względu na większe tłumienie punkty dostępowe wykorzystujące tą częstotliwość zapewniają mniejszy zasięg w pomieszczeniach (mimo zwiększenia dopuszczalnej mocy nadawania do 1 W), co z kolei wymusza zwiększenie zagęszczenia punktów dostępowych, które jako sąsiadujące ze sobą powinny pracować na różnych kanałach. Punkty dostępowe mogą wykorzystywać standardowe kanały wewnętrzne (nr od 36 do 48) oraz kanały zewnętrzne (od 52 do 144) z ograniczeniami związanymi z regulacjami prawnymi określonymi w danych krajach. Dodatkowo należy podkreślić, iż ze

względu na wykorzystywanie części tego pasma przez radary, dla tzw. kanałów zewnętrznych wymagane jest wsparcie przez stosowane urządzenia mechanizmu DFS (*ang. Dynamic Frequency Selection*), który pozwala na przełączenie się na inny kanał w przypadku wykrycia na nim jakiegoś sygnału. W praktyce oznacza to, iż kanał taki nie może być wykorzystany do obsługi użytkowników.

W celu zwiększenia prędkości z jaką można przesyłać dane, w różnych standardach możliwe jest łączenie ze sobą sąsiednich kanałów tworząc tym samym kanały o szerokim pasmie. W przypadku standardu 802.11n mamy możliwość korzystania z kanałów o szerokości 20 i 40 MHz, a w przypadku 802.11ac o szerokości 20, 40, 80, a nawet 160 MHz. Należy tutaj z całą stanowczością podkreślić, że ma to sens tylko w przypadku, gdy w wykorzystywanych kanałach nie mamy silnych zakłóceń, w tym sygnałów pochodzących z innych sieci.

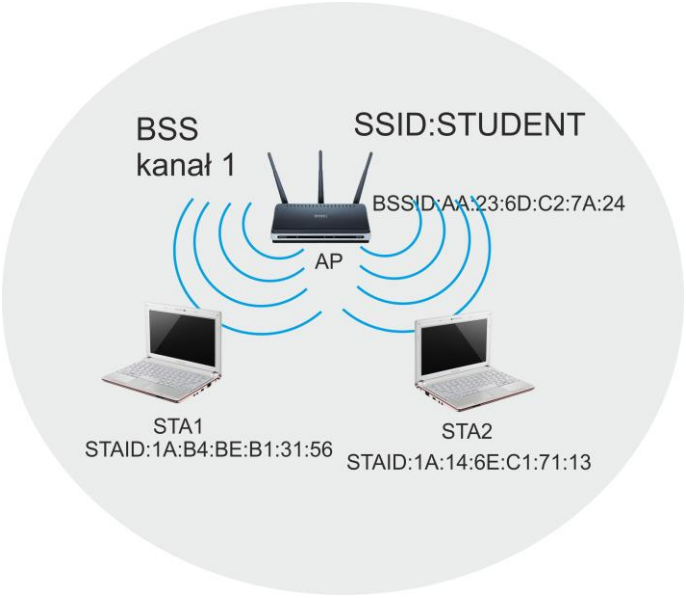
W celu zilustrowaniu tego problemu na Rysunku 5 przedstawiono ekran programu inSSIDer firmy MetaGeek [5] pozwalający użytkownikowi końcowemu przeskanować dostępne pasmo 2,4 GHz oraz 5 GHz w poszukiwaniu dostępnych sieci. Jak widać mamy tutaj do czynienia z sytuacją, w której widocznych jest bardzo dużo zakłócających się sieci. Co więcej administratorzy sieci o rozgłaszanych nazwach SSID: KROLIK, Dom 77 oraz TP-LINK_AEB69E zdecydowali się na pracę w kanale o szerokości 40 MHz, który powstał na skutek połączenia dwóch standardowych kanałów o szerokości 20 MHz (1+5). Oznacza to, że pierwszym w pełni separowalnym kanałem będzie dopiero kanał nr 10. Tym czasem nie dość, że wszystkie te wymienione sieci pracują w tym samym pasmie wzajemnie się zakłócając, to oprócz tego w 20 MHz kanałach o numerach od 1 do 9 pracuje jeszcze ponad pięć innych sieci. Jak widać z przedstawionej sytuacji, brak zrozumienia sposobu działania sieci bezprzewodowej podczas jej konfiguracji może znacząco wpłynąć na słabą jakość połączenia. Wybór domyślnego maksymalnego 40 MHz kanału dla sieci pracującej w standardzie 802.11n w tym przypadku na pewno nie okazał się odpowiedni. Ze względu na duże zaszumienie pasma 2,4 GHz użytkownicy pracujący w standardzie 802.11n powinni wykorzystać zupełnie wolne pasmo 5 GHz.



Rysunek 5. Przykład dostępnych sieci radiowych w środowisku domowym dla klienta w paśmie 2,4 GHz.

4. Podstawy funkcjonowania sieci bezprzewodowych

Podstawowym elementem sieci bezprzewodowej pracującej w standardzie 802.11 w trybie infrastruktury jest komórka sieci bezprzewodowej BSS (*ang. Basic Service Set*), składająca się z punktu dostępowego AP (*ang. Access Point*) oraz przynajmniej jednej stacji klienckiej STA (*ang. Station*), co zostało przedstawione na Rysunku 6. Każde z urządzeń w takiej sieci rozpoznawane jest na podstawie swojego unikalnego 48 bitowego adresu nazywanego dla punktów dostępowych BSSID (określającego jednocześnie identyfikator dla obsługiwanego BSS, stąd jego nazwa), a dla stacji klienckich STAID. Punkt dostępowy w celu zarządzania urządzeniami klienckimi oraz rozgłaszania informacji o obsługiwanej sieci, cyklicznie (standardowo co 100 ms) wysyła ramkę nawigacyjną *(ang. beacon frame)*, która między innymi zawiera informacje o identyfikatorze sieci SSID, kanale na którym pracuje dana sieć oraz wspieranych prędkościach transmisji danych (Rysunek 7).



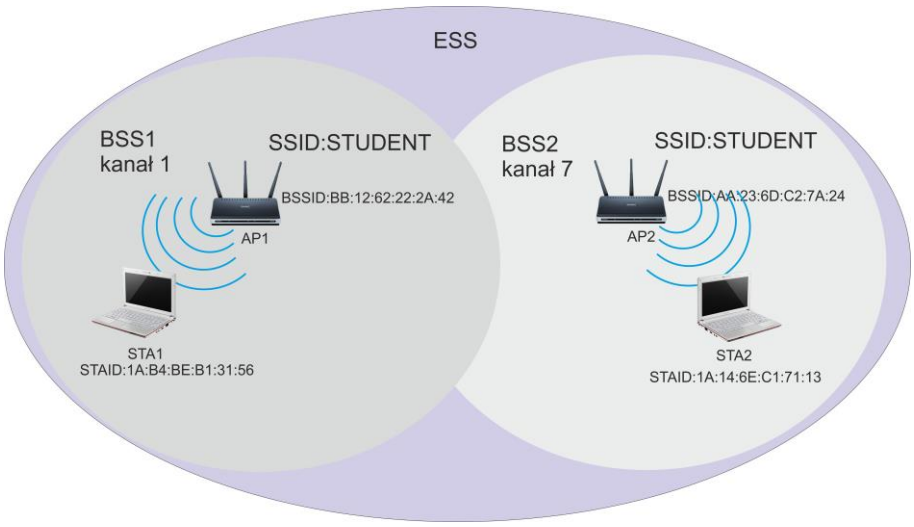
Rysunek 6. Podstawowa komórka sieci bezprzewodowej BSS ze zdefiniowaną nazwą sieci STUDENT (SSID), z widocznym identyfikatorem BSSID punktu dostępowego AP oraz identyfikatorami STAID dwóch stacji klienckich (STA1, STA2).

```
⊞ IEEE 802.11 Beacon frame, Flags: ........
⊟ IEEE 802.11 wireless LAN management frame
  ⊟ Fixed parameters (12 bytes)
      Timestamp: 0x000000005ca7c8e9
      Beacon Interval: 0.104448 [Seconds]
    ⊞ Capabilities Information: 0x0411
  ⊟ Tagged parameters (222 bytes)
    ⊞ Tag: SSID parameter set: TestSSID
    ⊞ Tag: Supported Rates 1, 2, 5.5(B), 6, 9, 11, 12, 18, [Mbit/sec]
    ⊞ Tag: DS Parameter set : Current Channel: 1
    ⊞ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ⊞ Tag: Country Information: Country Code US, Environment Any
    ⊞ Tag: QBSS Load Element 802.11e CCA Version
    ⊞ Tag: ERP Information: no Non-ERP STAs, do not use protection, long preambles
    ⊞ Tag: HT Capabilities (802.11n D1.10)
    ⊞ Tag: RSN Information
    ⊞ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ⊞ Tag: Reserved tag Number
    ⊞ Tag: Cisco CCX1 CKIP + Device Name
    ⊞ Tag: Cisco Unknown 96: Tag 150 Len 6
    ⊞ Tag: Vendor Specific: Microsof: WME
    ⊞ Tag: Vendor Specific: Aironet: Aironet Unknown
    ⊞ Tag: Vendor Specific: Aironet: Aironet CCX version = 5
    ⊞ Tag: Vendor Specific: Aironet: Aironet Unknown
    ⊞ Tag: Vendor Specific: Aironet: Aironet Unknown
```

Rysunek 7. Pola przykładowej ramki nawigacyjnej beacon.

Ze względu na ograniczenie zasięgu sieci bezprzewodowej w celu zwiększenia obszaru, na którym ma ona być dostępna, należy zastosować kolejne punkty dostępowe. Jeżeli pracują one w swoim bezpośrednim sąsiedztwie powinny zostać uruchomione

na niezakłócających się kanałach (np. 1 i 7). Punkty dostępowe rozgłaszające ten sam identyfikator (np. SSID:STUDENT) tworzą rozszerzoną komórkę ESS (*ang. Extended Service SET*), co zostało pokazane na Rysunku 8.



Rysunek 8. Rozszerzona komórka sieci bezprzewodowej ESS.

Ze względu na stosowaną technologię, sieci bezprzewodowe działają bardzo podobnie jak sieci Ethernet oparte na koncentratorach wieloportowych pracujące w trybie komunikacji jednokierunkowej (*ang. half-duplex*). W przypadku gdy wszystkie urządzenia korzystają ze wspólnej magistrali danych, do zarządzania wspólnym pasmem wykorzystywany jest mechanizm CSMA/CD (ang. *Carrier Sense Multiple Access / with Collision Detection*)[1]. Czytelnicy pragnący poszerzyć swoją wiedzę w zakresie sposobu działania sieci przewodowych mogą na przykład sięgnąć do wcześniejszych publikacji jednego z autorów niniejszego opracowania [8,9,10,11].

Podsumowując, sieć Ethernet można w skrócie scharakteryzować w następujący sposób:

- sieć działa w oparciu rozgłoszenia,
- urządzenia rozpoznawane są na podstawie adresu fizycznego MAC,
- wykorzystywany jest mechanizm zarządzania pasmem CSMA/CD implementowany na stacjach klienckich – brak urządzenia zarządzającego klientami,
- transmisja jest jednokierunkowa (half-duplex), co oznacza, iż tylko jedna stacja może nadawać w określonym czasie,

- urządzenie może rozpocząć nadawanie po upewnieniu się, że medium nie jest wykorzystywane do transmisji,
- w przypadku nadawania dwóch stacji w tym samym czasie pojawi interferencja sygnałów, która będzie interpretowana przez stacje jako kolizja,
- stacja, która zauważy kolizję wysyła sygnał o kolizji (*ang. jam signal*), który informuje pozostałych użytkowników o konieczności zaprzestania nadawania,
- po otrzymaniu sygnału o kolizji, stacje wstrzymują nadawanie i losują czas, po którym będą ponownie mogły rozpocząć nadawanie,
- nie ma określonej kolejności nadawania przez poszczególne stacje,
- pojedyncza ramka wypełnia cały segment sieci,
- pomiędzy wysyłanymi ramkami istnieje przerwa międzyramkowa IFG (*ang. Inter Frame Gap*) umożliwiająca innym użytkownikom skorzystanie z medium.

W przypadku sieci bezprzewodowej ze względu na fakt, iż dane wysyłamy drogą radiową i wszystkie urządzenia wykorzystujące określoną częstotliwość (kanał) mogą je odczytać, mamy sytuacją bardzo zbliżoną do Ethernetu. W skrócie można ja opisać w następujący sposób:

- sieć działa w oparciu rozgłoszenia,
- urządzenia rozpoznawane są na podstawie adresu fizycznego BSSID,
- wykorzystywany jest mechanizm zarządzania pasmem CSMA/CD (*ang. Carrier Sense Multiple Access / with Collision Avoidance*) nadzorowany przez punkt dostępowy, który zarządza podłączonymi urządzeniami klienckimi przydzielając im czas transmisji w celu unikania kolizji,
- najczęściej transmisja jest jednokierunkowa (half-duplex), co oznacza, iż tylko jedna stacja może nadawać w określonym czasie na jednej częstotliwości (kanale),
- urządzenie może rozpocząć nadawanie po upewnieniu się, że medium nie jest wykorzystywane do transmisji w czasie przydzielonym przez punkt dostępowy,
- w przypadku nadawania dwóch stacji w tym samym czasie pojawi interferencja sygnałów, która będzie prowadziła do błędów w transmisji,
- kolejność nadawania przez poszczególne stacje jest określana przez punkt dostępowy,

- pojedyncza ramka Wi-Fi nie koniecznie dociera do wszystkich klientów (problem ukrytego klienta),
- stacja kliencka może mieć przydzielony czas wykorzystania pasma lub możliwość wysłania/odebrania konkretnej ilości danych, mechanizm ten jest bardzo istotny przy stacjach klienckich pracujących z różnymi prędkościami transmisji,
- prędkość transmisji jest negocjowana z punktem dostępowym na podstawie jakości sygnału,
- funkcja DCF (*ang. Distributed coordination function*) pozwala na określenie priorytetu ruchu (ruch zarządzający jest ważniejszy od ruchu danych) oraz zapewnia wysyłanie potwierdzeń po każdej przesłanej ramce,
- wysyłane dane wymagają przesłania potwierdzenia (ACK).

Ze względu na niezbędny do prawidłowego funkcjonowania sieci bezprzewodowej ruch zarządzający, kontrolny, mechanizmy potwierdzenia otrzymania danych, szacuje się, że ostatecznie tylko 50% wynegocjowanego pasma może być wykorzystane do przesyłania właściwych danych.

5. Podłączanie klienta do sieci bezprzewodowej

W celu podłączenia do sieci bezprzewodowej stacja kliencka musi poznać jej parametry konfiguracyjne oraz minimalne wymagania. W tym celu klient próbuje rozpoznać dostępne sieci bezprzewodowe, określając jednocześnie wszystkie niezbędne informacje. Wykorzystywane są dwa sposoby wyszukiwania sieci:

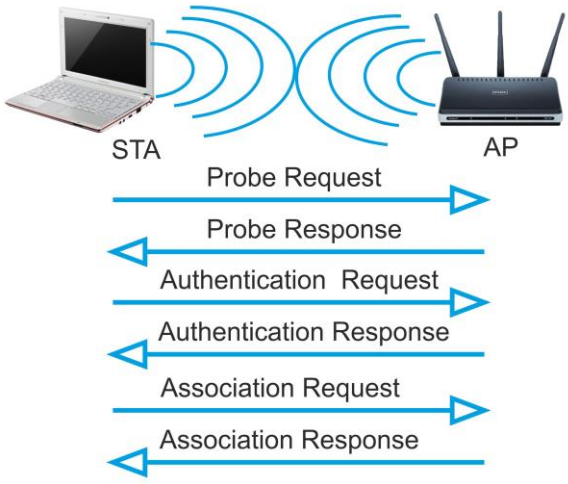
- Pasywne
    - Stacja skanuje poszczególne kanały radiowe, oczekując ramki nawigacyjnej (beacon) rozsyłanej przez AP.
    - W ramce nawigacyjnej przesyłane są parametry sieci takie jak: SSID, nr kanału radiowego, wspierane prędkości transmisji danych.
    - Stacja wśród nazw SSID uzyskanych z odebranych ramek szuka zapamiętanej nazwy. W przypadku znalezienia takiej sieci, stacja podejmuje próbę połączenia się z zapamiętaną siecią.
    - Jeżeli stacja nie znajdzie zapamiętaj sieci, oczekuje na wybór użytkownika.
- Aktywne

- Stacja wysyła ramkę typu Probe Request, zawierającą zapamiętany SSID sieci, z którą chce się połączyć, czasami stacja może wysłać Broadcast SSID.
- Po wysłaniu danych stacja kliencka oczekuje na odpowiedź Probe Response z punktu dostępowego.

Należy zaznaczyć, iż w trybie pasywnym ramki nawigacyjne rozgłaszane są przez sieć bezprzewodową z najmniejszą obsługiwaną prędkością transmisji. Działanie takie ma na celu zapewnienie tego, że zostaną one odebrane przez wszystkie urządzenia bez względu na obsługiwane prędkości transmisji. Rozwiązanie takie jednakże negatywnie wpływa na wydajność sieci ze względu na zajmowany przez te ramki czas radiowy. W związku z powyższym, w celu optymalizacji sieci zalecane jest wyłączenie na punkcie dostępowym obsługi najmniejszych prędkości transmisji.

Kolejnym etapem jest proces autentykacji. W odróżnieniu od autentykacji sieciowej, weryfikowana jest jedynie zgodność urządzenia klienta z punktem dostępowym (Authentication Request, Authentication Response). Wyróżnia się dwa warianty autentykacji:

- Otwarta - brak weryfikacji klienta, używana w połączeniu z autentykacją sieciową 802.1x/EAP.
- Z kluczem współdzielonym wykorzystująca WEP, podczas której sprawdzana jest zgodność obu kluczy.



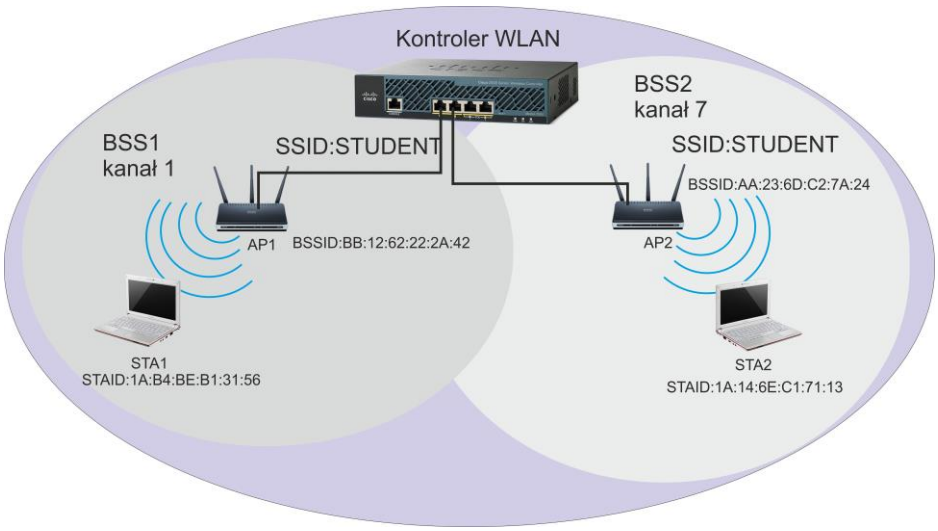
Rysunek 9. Etapy przyłączania klienta do sieci bezprzewodowej.

Po etapie autentykacji następuje asocjacja, mająca na celu uczynienie klienta pełnoprawnym członkiem BSS. Autentykacja następuje po wysłaniu przez klienta ramki Association Request. W przypadku zgody na podłączenie się do sieci klient otrzymuje ramkę Association Response z unikalnym numerem AID przypisywanym przez sieć dla każdego podłączonego klienta.

Po tych obowiązkowych etapach przyłączenia do sieci, mogą (w zależności od konfiguracji sieci) nastąpić kolejne procesy np. realizujące autoryzację w oparciu o WPA2. Po pomyślnym zakończeniu tych etapów, klient może rozpocząć procedurę automatycznej konfiguracji interfejsu sieciowego w oparciu o protokół DHCP, którego opis można znaleźć w różnych opracowaniach [8]. Po otrzymaniu niezbędnych danych konfiguracyjnych (adres IP, maska, brama), klient staje się pełnoprawnym członkiem sieci.

6. Zarządzanie punktami dostępowymi

Zarządzanie rozległymi sieciami bezprzewodowymi, złożonymi z wielu punktów dostępowych, nastręcza wiele trudności, a w przypadku ich skomplikowanej konfiguracji może okazać się wprost niemożliwe. W celu rozwiązania tego problemu, administratorzy coraz częściej rezygnują z sieci bezprzewodowych opartych na autonomicznych punktach dostępowych (tzw. *Fat APs*), wybierając rozwiązania oparte na kontrolerach WLC (*ang. Wireless Controller*), co przedstawiono na Rysunku 10.



Rysunek 10. Sieć bezprzewodowa oparta na kontrolerze.

W takim podejściu pełna kontrola spoczywa na urządzeniu określanym jako kontroler sieci bezprzewodowych, a punkty dostępowe stają się jedynie prostymi urządzeniami nadawczo-odbiorczymi (tzw. *Thin APs*). W zależności od przyjętego rozwiązania kontroler może zarządzać punktami dostępowymi znajdującymi się w jego sieci lokalnej, może znajdować się w zdalnej lokalizacji lub wręcz być oprogramowaniem pracującym na serwerach wirtualnych znajdujących się w chmurze. Rozwiązania oparte na kontrolerach cechuje znacznie większe bezpieczeństwo niż rozwiązania wykorzystujące autonomiczne punkty dostępowe, gdyż w tym pierwszym przypadku AP nie posiada żadnych poufnych informacji, a decyzja o autentykacji klienta podejmowana jest przez kontroler. W związku z powyższym, w przypadku fizycznej kradzieży sprzętu złodziej nie będzie posiadał żadnych danych dotyczących konfiguracji sieci bezprzewodowej.

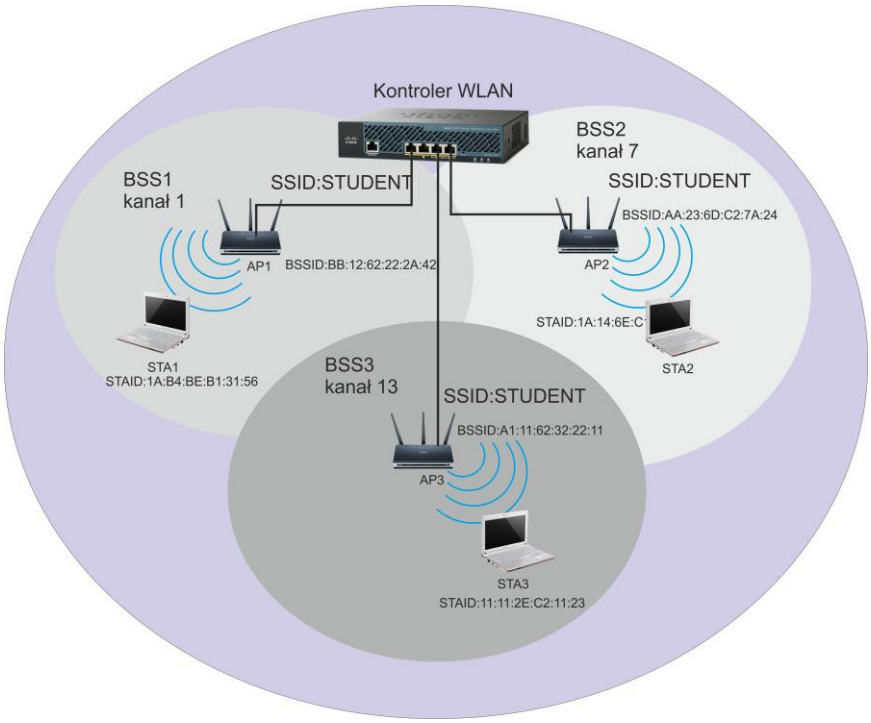
Wykorzystanie tego typu rozwiązań bez wątpienia ułatwia zarządzanie siecią, pozwalając na przykład na automatyczny dobór mocy poszczególnych interfejsów radiowych w celu zapewnienia maksymalnego obszaru pokrycia siecią. Czasami kontrolery pozwalają również na automatyczny dobór niezakłócających się kanałów radiowych dla poszczególnych punktów dostępowych. Ponadto przy zastosowaniu odpowiedniego oprogramowania możliwe jest określanie fizycznej lokalizacji użytkowników. Niestety rozwiązania te nie eliminują wszystkich problemów związanych z dużymi sieciami bezprzewodowymi.

7. Meru Networks: wirtualna komórka i wirtualny port

Jednym z problemów typowej sieci bezprzewodowej jest obsługa mobilnych klientów. Przechodząc z obszaru obsługiwanego przez jeden punkt dostępowy do obszaru obsługiwanego przez inny punkt dostępowy ulegają oni rozłączeniu, a następnie ponownemu przyłączeniu. Dzieje się tak nawet w przypadku, gdy punkty dostępowe rozgłaszają taki sam SSID oraz korzystają z tego samego kanału. Należy przypomnieć, iż każdy z punktów dostępowych identyfikuje się swoim unikalnym numerem BSSID, który pozwala klientowi odróżnić od siebie dostępne punkty dostępowe. Proces przełączania klienta odbywa się w następujących etapach:

1. Karta klienta stale kontroluje jakość sygnału radiowego,
2. Gdy poziom sygnału spadnie poniżej dopuszczalnego poziomu, karta przechodzi w tryb skanowania i zaczyna wyszukiwać silniejsze źródło sygnału,
3. Po znalezieniu odpowiedniego sygnału zapada decyduje o przełączeniu,
4. Następuje zerwanie połączenia, jeśli to konieczne, to zmiana kanału, a następnie podłączenie do nowego punktu dostępowego.

Proces ten trwa od 50 do 3000 ms, co oznacza, iż pomimo uzyskania przez klienta tego samego adresu IP, część połączeń sieciowych zostanie w tym czasie rozłączonych. O momencie przełączenia pomiędzy punktami dostępowymi decyduje karta bezprzewodowa klienta. Z powodu nieposiadania przez kartę klienta wiedzy o obciążeniu i funkcjonowaniu sieci, przełączanie takie może okazać się nieoptymalne. Nawet w przypadku rozwiązań opartych na kontrolerze, nie istnieje możliwość wskazania klientowi odpowiedniego, preferowanego AP, a możliwe jest jedynie zakończenie istniejącej sesji.

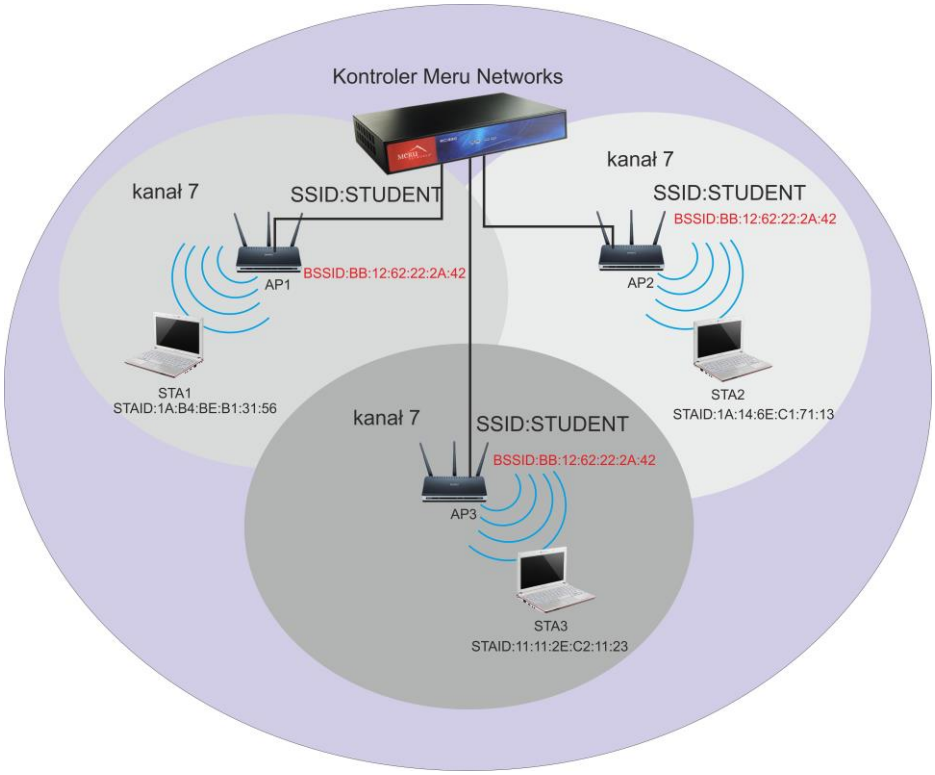


Rysunek 11. Typowa topologia dla sieci składającej się z trzech punktów dostępowych, wykorzystywane kanały radiowe 1,7 i 13.

Problem różnych identyfikatorów BSSID w obrębie jednej sieci eliminuje mechanizm **wirtualnej komórki** (*ang. Virtual Cell*) proponowanej w rozwiązaniach Meru Networks. W odróżnieniu od typowej sieci bezprzewodowej (Rysunek 11), wszystkie punkty dostępowe pracują na tym samym kanale radiowym i wysyłają ramki z tym samym identyfikatorem BSSID (Rysunek 12). Oznacza to, że pomimo, iż w sieci możemy mieć kilka punktów dostępowych, klient nie potrafi ich rozróżnić, traktując otrzymywane ramki tak, jakby były wysyłane przez pojedyncze urządzenie. W związku z powyższym, przy zmianie swojej lokalizacji klient nie podejmuje próby przełączania, a jedynie jest „przekazywany" przez kontroler pomiędzy kolejnymi punktami dostępowymi. Oczywiście w tym przypadku kontroler dba o to, aby ramki kierowane

do stacji klienta były przesyłane przez aktualnie obsługujący go punkt dostępowy. Oznacza to, że kontroler w sposób ciągły monitoruje sieć i sprawdza, który z punktów dostępowych najlepiej nadaje się do obsługi klienta, uwzględniając bieżące obciążenia sieci i jakości sygnału. Proces przełączania w takiej sieci jest natychmiastowy (do 3ms), niezauważalny dla klientów, a co najważniejsze nie powoduje przerwy w dostępie do sieci.

Kolejną bardzo ważna zaletą tej technologii jest łatwa możliwość rozbudowy sieci o kolejne punkty dostępowe. Ze względu na fakt, iż na wszystkich punktach dostępowych wykorzystywany jest ten sam kanał radiowy, rozszerzenie sieci o kolejne urządzenia polega wyłącznie na podłączeniu nowego AP do kontrolera bez potrzeby analizowania dostępnego kanału radiowego, który nie będzie wpływał na zakłócenia istniejących już punktów dostępowych. W ramach tak przygotowanej jednej fizycznej sieci bezprzewodowej można rozgłaszać różne identyfikatory sieciowe SSID, co oznacza, iż klienci mogą podłączać się do różnych rozgłaszanych sieci, wykorzystujących różne autentykacje i dające różny dostęp do zasobów, które fizycznie obsługiwane są przez ten sam kontroler i punkty dostępowe. Rozwiązanie takie w sposób znaczący ułatwia konfigurację i zarządzanie siecią bezprzewodową.



Rysunek 12. Topologia wirtualnej komórki wykorzystująca jeden identyfikator BSSID oraz jeden kanał radiowy na obszarze całej sieci bezprzewodowej.

Rozszerzeniem technologii wirtualnej komórki jest **wirtualny port** (*ang. Virtual port*). W trybie tym kontroler generuje na podstawie identyfikatora STAID klienta unikany identyfikator wirtualnego punktu dostępowego BSSID, z którym będzie komunikował się klient. Dzięki temu rozwiązaniu każdy klient jest indywidualnie obsługiwany przez jeden wirtualny punkt dostępowy, który może w pełni zoptymalizować parametry transmisji dla swojego klienta. W przypadku klasycznego rozwiązania, ramki nawigacyjne wysyłane są do wszystkich obsługiwanych klientów. W praktyce oznacza to, że podłączone do kontrolera punkty dostępowe są w stanie wysyłać dane na tym samym kanale przedstawiając się różnymi identyfikatorami BSSID. Ponadto w przypadku transmisji szyfrowanej w trybie tym współdzielone klucze WPA są unikalne dla każdego klienta, co znacznie zwiększa poziom bezpieczeństwa. Identyfikator BSSID wirtualnego punktu dostępowego przypisany do danego użytkownika nie ulega zmianie w trakcie przełączania klienta pomiędzy różnymi punktami dostępowymi.

Praca w trybie wirtualnej komórki umożliwia również efektywniejsze wykorzystanie pasma radiowego ze względu na wbudowane zarządzanie interferencjami wewnątrzkanałowymi. Oznacza to, że sieć taka zabezpieczona jest przed zakłóceniami pochodzącymi od własnej infrastruktury. Ponadto ze względu na fakt, iż wszystkie punkty dostępowe wykorzystują jeden kanał radiowy, niepotrzebne jest skomplikowane planowanie użycia różnych kanałów radiowych w celu uniknięcia zakłóceń, a rozszerzenie sieci wymaga po prostu podłączenia kolejnego punktu dostępowego do kontrolera

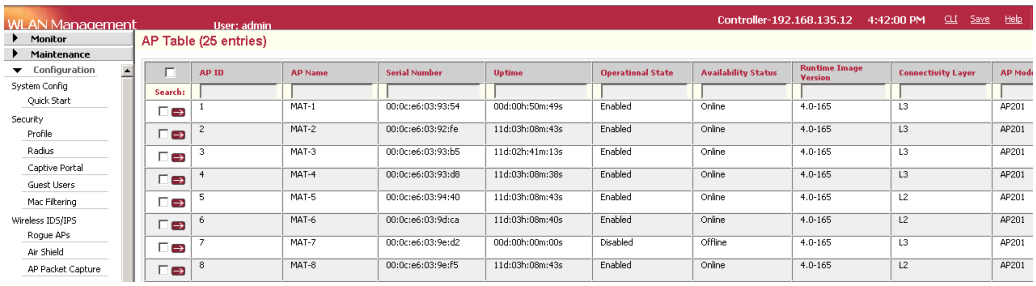
8. Konfiguracja sieci Wi-Fi w oparciu o kontroler Meru

Infrastruktura sieci bezprzewodowej Meru Networks składa się z kontrolera oraz jednego lub więcej punktów dostępowych. Zarządzanie kontrolerem możliwe jest przy wykorzystaniu połączenia konsolowego za pomocą interfejsu szeregowego lub sesji ssh. Ponadto istnieje również możliwość wykorzystania przeglądarki internetowej obsługującej protokół https.

Aby móc uruchomić sieć bezprzewodową, muszą być spełnione następujące warunki:

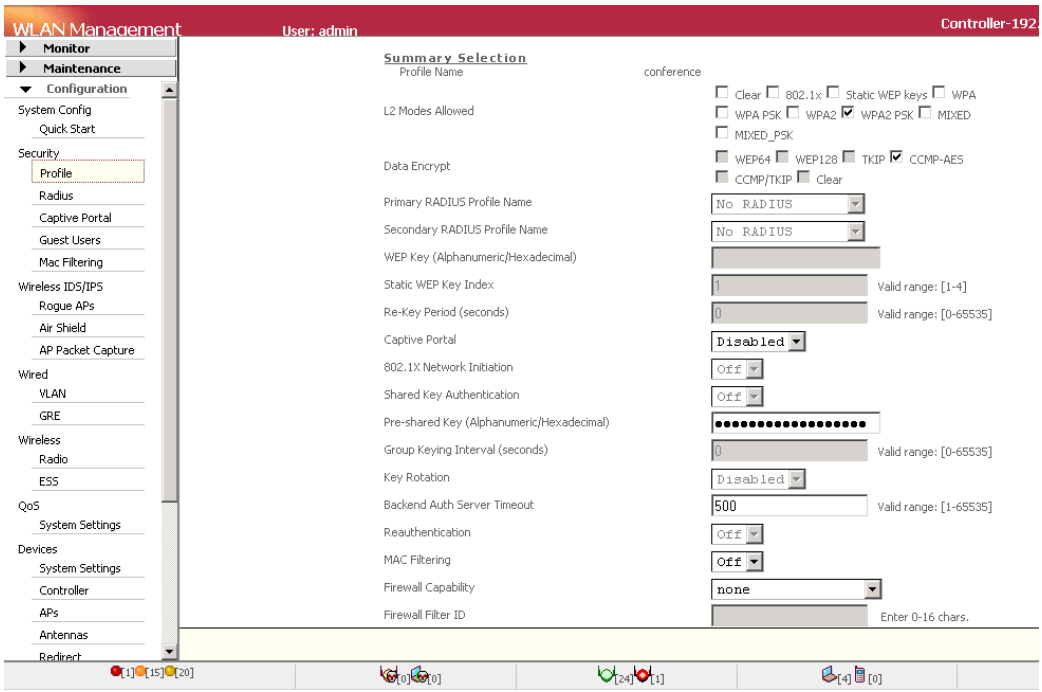
- Kontroler i punkty muszą mieć zapewnioną możliwość nawiązania połączenia w warstwie 2 lub 3 modelu OSI,
- W przypadku wykorzystania warstwy 3 AP musi mieć przydzielony adres IP, a jeśli adres ten należy do innej sieci niż adres kontrolera, musi zostać uruchomiony routing między tymi sieciami.

Po podłączeniu punktu dostępowego do sieci, próbuje on nawiązać łączność z kontrolerem. Po jej nawiązaniu punkt dostępowy pojawia się na liście urządzeń zarządzanych przez kontroler.



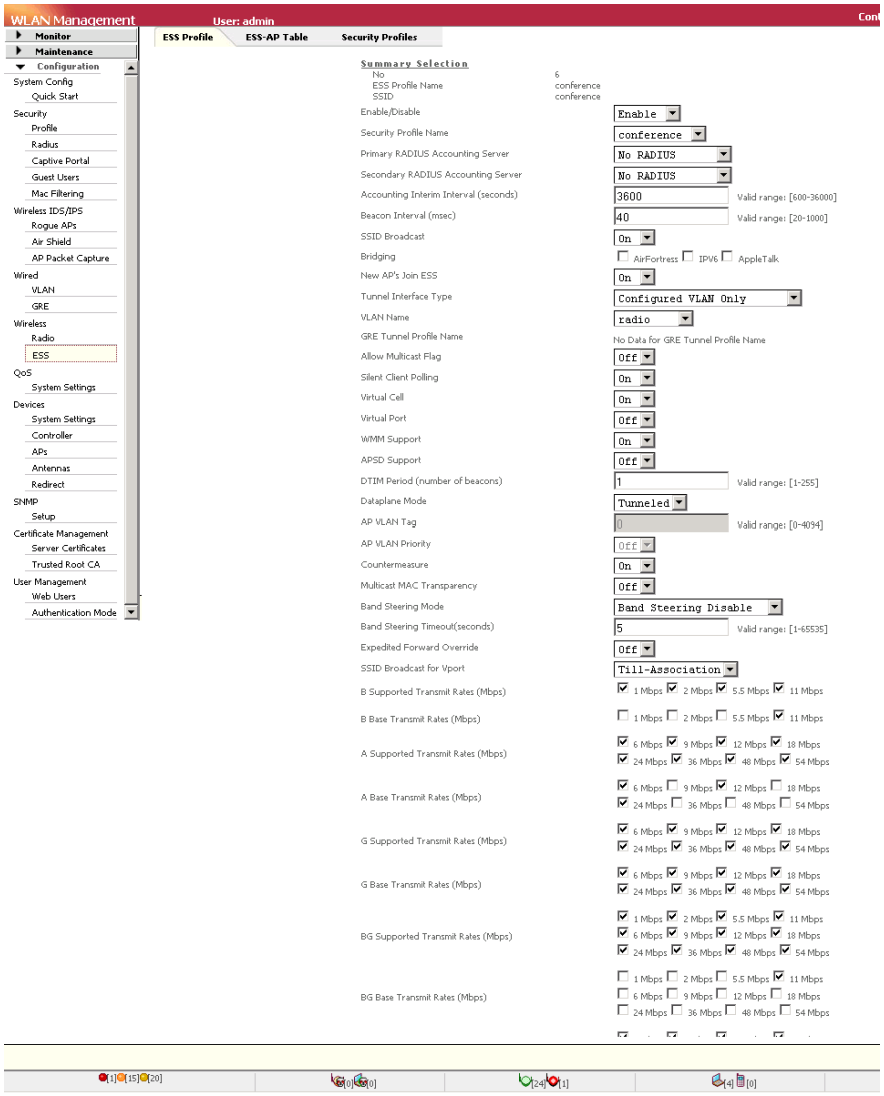
Rysunek 13. Lista podłączonych punktów dostępu.

Konfigurację nowej sieci bezprzewodowej należy rozpocząć od stworzenia profilu bezpieczeństwa (*ang. Security Profile*). Na tym etapie należy zdecydować między innymi o sposobie uwierzytelniania, wskazać serwer radius, zdefiniować hasło do sieci itp. Możliwe opcje zostały przedstawione na Rysunku 14.



Rysunek 14. Okno tworzenia profilu bezpieczeństwa.

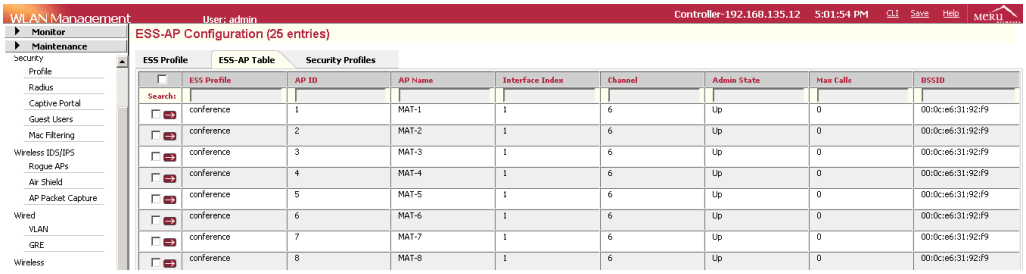
Kolejny krok polega na stworzeniu profilu ESS. Na tym etapie należy zdefiniować SSID tworzonej sieci, jej dostępność, wybrać jeden ze zdefiniowanych uprzednio profili bezpieczeństwa, zdecydować o VLAN-ie, do którego będą przyłączani klienci, a także włączyć opcję wirtualnej komórki oraz wirtualnego portu. Ponadto można również określić jakie prędkości transmisji będą dostępne w każdym z obsługiwanych standardów.



Rysunek 15. Tworzenie nowego profilu sieci.

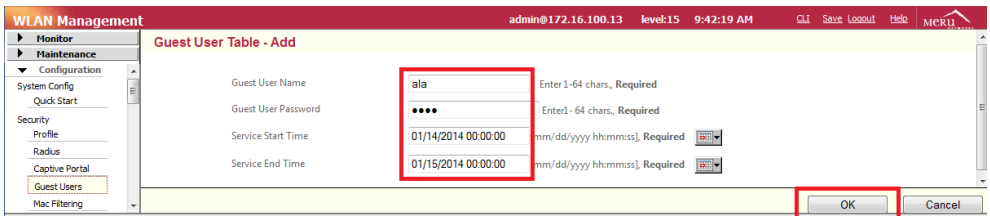
Po wykonaniu tych kroków, zdefiniowana sieć bezprzewodowa zaczyna być rozgłaszana przez wszystkie punkty dostępowe zarządzane przez konfigurowany kontro-

ler. W przypadku potrzeby włączenia lub wyłączenia obsługi konkretnej sieci przez konkretny punkt dostępowy możliwe jest to za pomocą zakładki ESS-AP Table. Tak jak to zostało już powiedziane, pojedynczy punkt dostępowy może obsługiwać wiele sieci radiowych równocześnie. W domyślnej konfiguracji nowo tworzona sieć jest obsługiwana przez wszystkie punkty dostępowe podłączone do kontrolera.

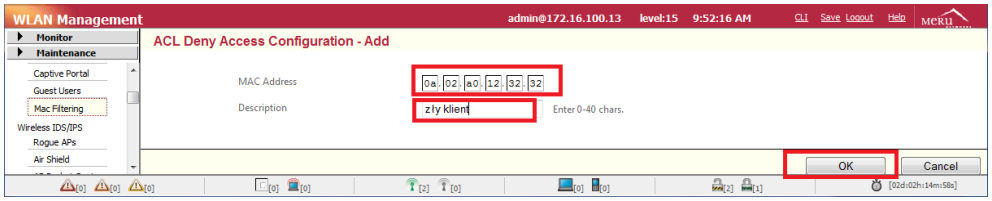


Rysunek 16. Lista AP przewidzianych do obsługi nowej sieci.

Ponadto oprogramowanie kontrolera pozwala również na łatwy sposób tworzenia kont dostępowych dla gości przy wykorzystaniu wbudowanej funkcji Captive Portal. W przypadku takiego uwierzytelnienia klient po podłączeniu do sieci (autentykacja otwarta) zostanie przekierowany na stronę Captive Portal, na której zostanie poproszony o podanie loginu i hasła. Po prawidłowej autentykacji stacja kliencka stanie się pełnoprawnym użytkownikiem sieci bezprzewodowej. Należy zaznaczyć, iż każde zdefiniowane konto posiada własną nazwę, hasło oraz termin ważności. Dodatkowo możliwa jest autentykacja w oparciu o mechanizm list dostępowych oraz filtrowanie adresów MAC (STAID).



Rysunek 17. Tworzenie kont użytkowników korzystających z usługi Captive Portal.



Rysunek 18. Weryfikacja użytkowników z wykorzystaniem adresów MAC.

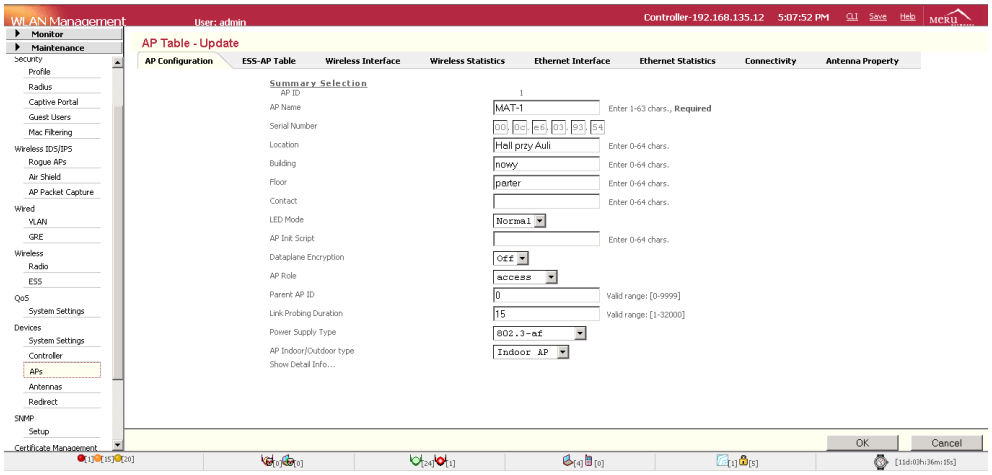
9. Zaawansowana konfiguracja kontrolera

Oprogramowanie kontrolera posiada wiele ustawień, które w podstawowej konfiguracji nie muszą być zmieniane. Obejmują one między innymi konfigurację: poszczególnych punktów dostępowych, mechanizmu QoS oraz Air Shield.

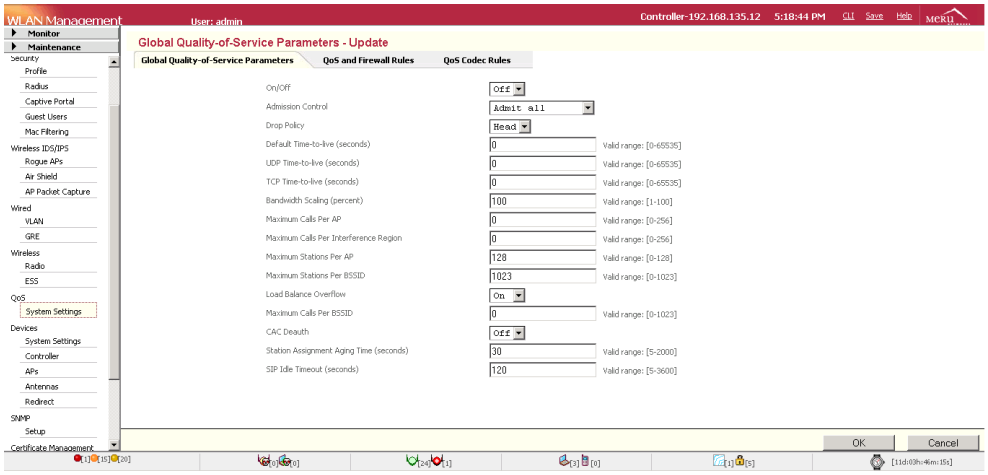
W przypadku zarządzanych punktów dostępowych możliwe jest indywidualne skonfigurowanie:

- Opisu i nazwy każdego urządzenia,
- Listy obsługiwanych sieci,
- Parametrów interfejsu bezprzewodowego i przewodowego,
- Parametrów anteny.

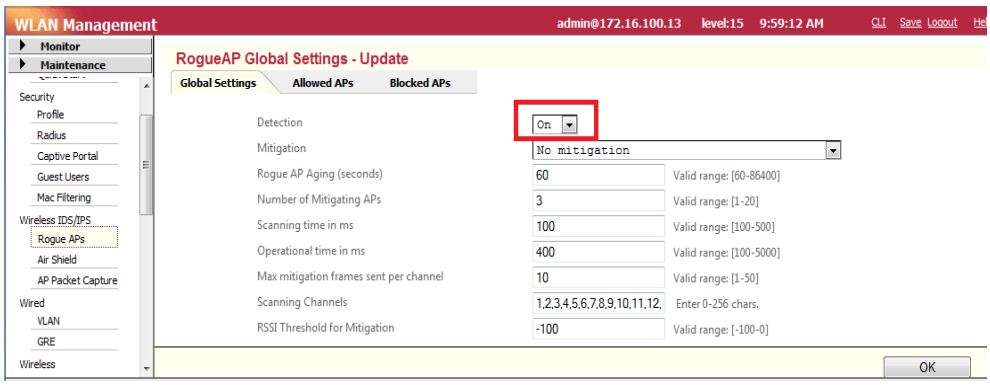
Każdy punkt posiada również własne narzędzia diagnostyczne i statystyki.



Rysunek 19. Okno konfiguracji AP.



Rysunek 20. Okno konfiguracji QoS.



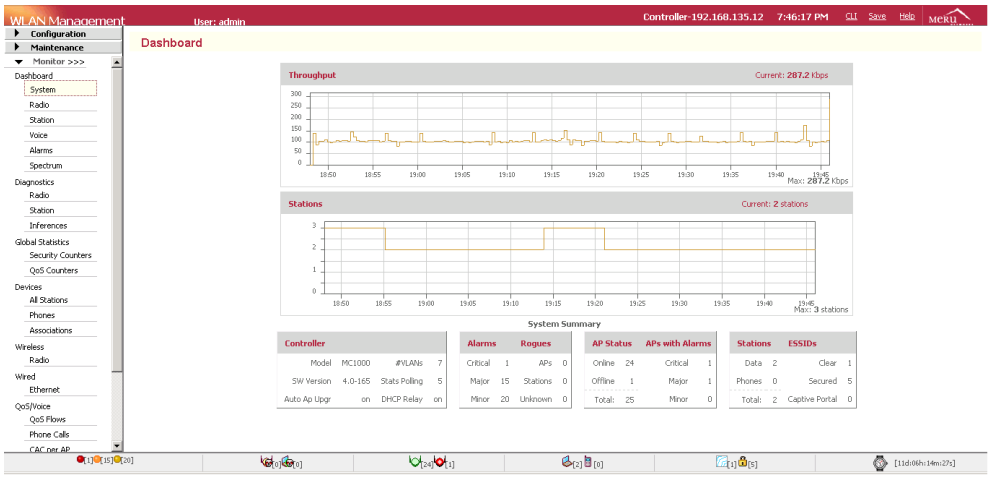
Rysunek 21. Wykrywanie obcych sieci i punktów dostępowych.

Kontroler posiada wbudowane mechanizmy mitygacji obcych sieci. Umożliwia on wykrywanie i blokowanie działania obcych sieci znajdujących się w zasięgu punktu dostępowego Meru Networks. Należy jednakże zachować ostrożność podczas korzystania z tej funkcji z powodu jej negatywnego wpływu na wydajność sieci.

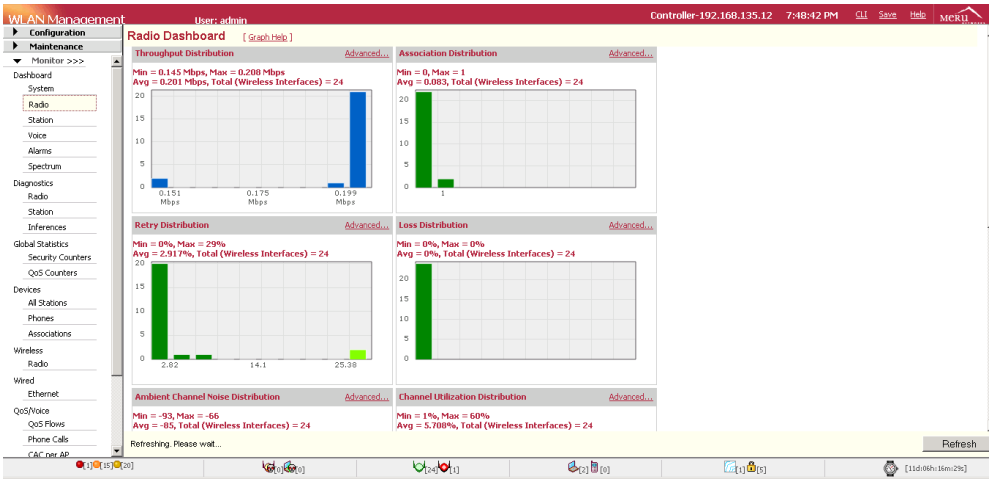
10. Analiza funkcjonowania sieci

Podczas zarządzania siecią bezprzewodową bardzo ważna jest możliwość monitoringu jej pracy. W przypadku oprogramowania kontrolera Meru Networks dostępna zakładka Monitor pozwala nadzorować działanie całej sieci bezprzewodowej, w tym:

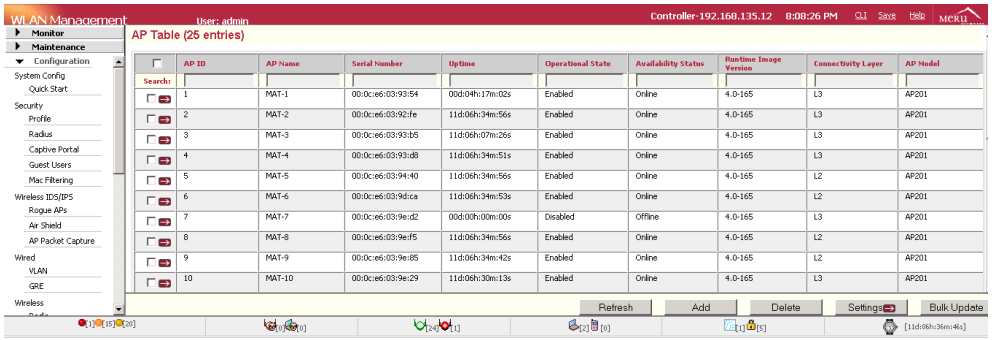
- Bieżące obciążenie sieci według punktów dostępowych i klientów,
- Liczbę obsługiwanych klientów,
- Informacje o klientach (nazwa sieci, ilość przesyłanych danych, jakość transmisji, przydzielone adresy, itp.),
- Listę asocjacji,
- Warunki radiowe,
- Dziennik zdarzeń,
- Informacje o obecności w zasięgu innych sieci,
- Informacje o funkcjonowaniu wszystkich punktów dostępowych.



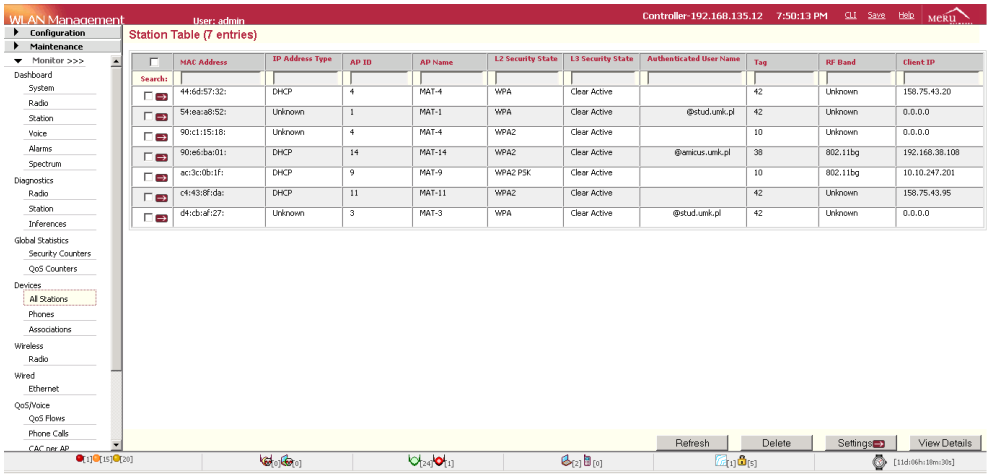
Rysunek 22. Zakładka stanu systemu.



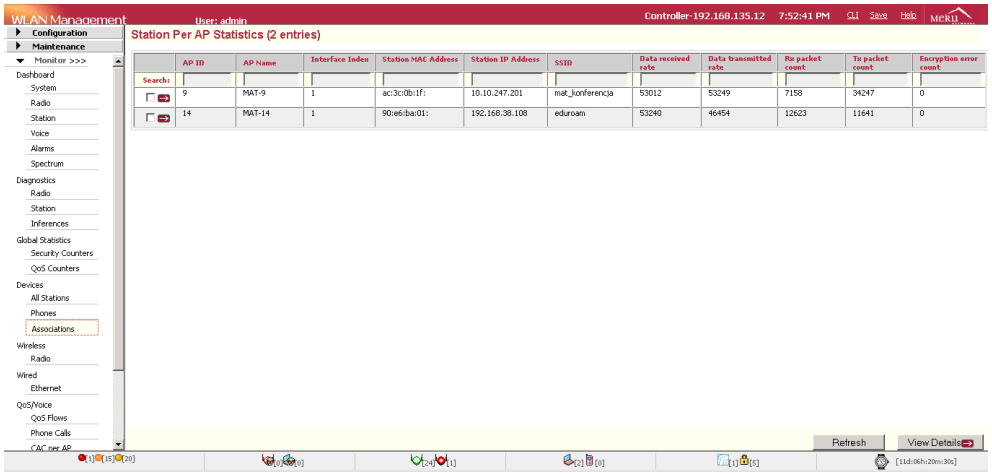
Rysunek 23. Zakładka z informacjami o warunkach radiowych.



Rysunek 24. Informacje o pracy AP.



Rysunek 25. Informacje o podłączonych stacjach.



Rysunek 26. Informacje o przyłączonych stacjach klienckich.

11. Podsumowanie

Celem niniejszego opracowania było przybliżenie czytelnikowi problematyki związanej z realizacją sieci bezprzewodowych, realizowanych zgodnie ze standardem IEEE 802.11. Opisane zostały również rozwiązania wykorzystujące kontrolery, umożliwiające globalne zarządzanie siecią bezprzewodową zbudowaną z wielu punktów dostępowych. Przedstawiono również technologię wirtualnej komórki oraz wirtualnego portu, które pozwalają na znaczne uproszczenie zarządzania siecią bezprzewodową oraz optymalizację udostępnianego klientowi pasma. Rozwiązanie to obecnie wydaje się być jednym z najbardziej zaawansowanych rozwiązań z zakresu zarządzania dużymi sieciami bezprzewodowymi. Wszystkie te aspekty spowodowały, że sieci Meru Networks zostały wybrane przez Cyfrową Szkołę jako najlepsze rozwiązanie sprawdzone w edukacji.

Literatura

1. http://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_detection
2. http://www.bluetooth.org/en-us
3. http://www.fen.pl/cyfrowaszkola
4. http://www.ieee.org/index.html
5. http:// www.metageek.net

6. http://www.wi-fi.org/
7. http://www.wimaxforum.org/
8. M. Piwiński, Automatyczna konfiguracja interfejsu sieciowego, czyli protokół DHCP w praktyce, Uczyć się będąc połączonym, 235-247, Teksty wystąpień, red. M. Sysło, A. B. Kwiatkowska, X Konferencja "Informatyka w Edukacji" 2013, Wydawnictwa Naukowe UMK, ISBN 978-83-231-3105-2, Toruń, 2013, http://repozytorium.umk.pl/handle/item/1729
9. M. Piwiński, How to teach computer networks using simulation software?, Learning while we are connected, Vol. 3, 242 Book of abstracts, red. N. Reynolds, M. Webb, M. Sysło, V. Dagiene, 10th World Conference on Computers in Education, 2013, Nicolaus Copernicus University Press, ISBN 978-83-231-3095-6, Toruń, 2013, http://repozytorium.umk.pl/handle/item/1775
10. M. Piwiński, Internet - wybrane aspekty bezpieczeństwa, Informatyka w Edukacji, Monografia naukowa, red. A.B. Kwiatkowska, Wydawnictwa Naukowe UMK, 2013, http://repozytorium.umk.pl/handle/item/1712
11. M. Piwiński, „Praktyczna analiza sieci komputerowych z wykorzystaniem programu Wireshark", „Informatyka w Edukacji, V", A.B. Kwiatkowska, M. Sysło, (2008) 277 285, http://repozytorium.umk.pl/handle/item/1686