Dlaczego Meru Networks – architektura jednokanałowa

- Architektura jednokanałowa:
  - Brak konieczności planowania kanałów i poziomów mocy na poszczególnych AP
  - Zarządzanie interferencjami wewnątrzkanałowymi, brak zakłóceń od własnej infrastruktury
  - Dokładniejsze pokrycie przy mniejszej ilości AP, nawet do 30 %

Meru (jeden kanał)	Tradycyjne sieci (mikrokomórka)
Brak konieczności planowania kanałów w obrębie infrastruktury	Konieczność planowania kanałów ręcznie lub automatycznie(algorytm może dodatkowo obciążać kontroler sieci bezprzewodowej)
Synchronizacja pracy AP i zarządzanie interferencjami wewnątrz kanału, brak zakłóceń od swoich AP	Konieczność zmniejszania mocy nadawania na AP, aby unikać interferencji wewnątrz kanału i zakłóceń pomiędzy swoimi AP
Możliwość wykorzystania pełnej mocy na AP, lepsze pokrycie przy zastosowaniu mniejszej ilości urządzeń, nawet do 30 %	Z reguły słabsze pokrycie i konieczność zastosowania większej ilości AP z powodu ograniczania mocy nadawania aby unikać interferencji

Dlaczego Meru Networks – Wirtualna komórka

- Wirtualna komórka Meru:
  - Cała infrastruktura widoczna jest dla klienta jako jeden AP
  - Decyzję o przełączeniu klienta podejmuje kontroler, biorąc pod uwagę jej wpływ na pracę reszty sieci
  - Niezauważalne dla klienta przełączanie pomiędzy AP, zapewnia ciągłość pracy dla nawet najbardziej wymagających aplikacji np. wideo

Meru Networks	Tradycyjne sieci
Wszystkie AP są widoczne dla karty bezprzewodowej jako jedno urządzenie, jeden bezprzewodowy MAC - BSSID	Każdy AP jest widoczny dla klienta pod swoim unikalnym identyfikatorem bezprzewodowym BSSID
Klient nie może podjąć decyzji o przełączeniu ponieważ dla niego istnieje tylko jeden wirtualny AP, dzięki temu kontroler może zdecydować czy przełączać klienta biorąc pod uwagę wpływ tej decyzji na resztę sieci i zapewnić balansowanie obciążeniem	Karta bezprzewodowa podejmuje decyzję o przełączeniu na bazie siły sygnału od aktualnego AP, oraz na podstawie widocznych innych BSSID(innych AP) pracujących na innych kanałach, kontroler może jedynie zdecydować o wyrzuceniu klienta z danego AP
Proces przełączenia jest dla klienta niezauważalny i zajmuje mniej niż 10 ms, dzięki temu karta bezprzewodowa nie zrywa transmisji co zapewnia niezakłóconą pracę nawet dla najbardziej wymagających aplikacji, z punktu widzenia klienta nie występuje zjawisko skakania między AP	Na proces przełączania składa się konieczność przełączenia karty na inny kanał radiowy, ponownego podłączenia do nowego AP i czasem ponownej autentykacji może to zająć od 50 do 3000 ms, jest zauważalne i może zakłócać pracę aplikacji, możliwe jest wystąpienie zjawiska skakania między AP, praktycznie uniemożliwiające normalną pracę

Dlaczego Meru Networks – Wirtualny Port

- Wirtualny Port Meru:
  - Sieć bezprzewodowa pracująca jak przełącznik - kierowanie transmisji tylko do konkretnego użytkownika
  - Zarządzanie parametrami transmisji na zasadzie per użytkownik
  - Większe bezpieczeństwo

Meru Networks	Tradycyjne sieci
Każdy klient podłączając się do sieci uzyskuje wirtualne i unikalne dla siebie BSSID, które od tej pory „podąża” za nim, tak jakby był podłączony do portu na przełączniku, transmisja jest kierowana tylko do konkretnego klienta	Każdy klient podłączając się do sieci widzi ogólne BSSID danego AP, BSSID zmienia się gdy klient się przemieszcza między AP, transmisja jest kierowana do wszystkich w obrębie danego BSSID, tak jakby klient był podłączony do jednego z wielu hubów
AP dzięki wykorzystaniu unikalnego BSSID dla każdego klienta może sterować parametrami transmisji i dopasowywać je do aktualnych możliwości danego użytkownika	AP poprzez wykorzystanie wspólnego BSSID nie może sterować parametrami transmisji per klient, stosuje więc jedne ustawienia dla wszystkich nie dopasowując się do konkretnego klienta
Dzięki wykorzystaniu unikalnego BSSID, klucz współdzielony WPA wysyłany na początku negocjacji zabezpieczeń jest unikalny dla każdego klienta, rozwiązuje to problem luki 196 w standardzie WPA	Z powodu wspólnego BSSID dla wszystkich, klient który podłączył się do sieci znając wspólny klucz może spróbować odszyfrować transmisję innych użytkowników, jest to problem luki 196 w standardzie WPA

Dlaczego Meru Networks – Air Time Fairness

- Air Time Fairness:
  - Możliwość równomiernego podziału dostępu do medium transmisyjnego
  - Ochrona przed spowolnieniem sieci przez wolniejszych użytkowników
  - Zapewnienie maksymalnej wydajności dla każdego podłączonego do AP

Meru Networks	Tradycyjne sieci
Technologia Air Time Fairness dzięki zastosowaniu czasowego podziału dostępu do medium bezprzewodowego zapewnia równomierny podział zasobu jakim jest „czas transmisji w powietrzu” pomiędzy wszystkich klientów, dzięki temu ograniczone jest zjawisko kolizji i konieczność ponawiania transmisji	Bez możliwości podziału „czasu transmisji w powietrzu” stacje bezprzewodowe rywalizują o dostęp do medium na zasadzie „kto pierwszy ten lepszy”, zjawisko kolizji występuje częściej, związane jest z koniecznością ponawiania transmisji co zmniejsza przepustowość całej sieci
Dzięki równomiernemu podziałowi, każdy użytkownik otrzymuje tyle samo czasu na transmisję, wolni użytkownicy nie mają możliwości zużycia całego dostępnego czasu tylko na swoje potrzeby	Tradycyjne systemy korzystają z podejścia „pakietowego” zamiast czasowego, przez co dzielą zasoby w zależności od tego ile kto ma danych do przesłania, to często powoduje zużycie większości pasma przez wolnych użytkowników pracujących np. w standardzie b lub znajdujących się większej odległości od AP
Podział czasowy daje jeszcze jedną zaletę, ponieważ każdy ma przydzielony określony czas, użytkownicy pracujący z większymi prędkościami mogą wysłać więcej danych niż pracujący wolniej, każdy pracuje więc ze swoją maksymalną wydajnością	Bez podziału czasowego, użytkownicy którzy mają coś do wysłania rywalizują o dostęp do medium, stacja pracująca z niższą prędkością a mająca dużo danych do wysłania zajmuje medium na dłużej niż stacja która może pracować szybko, przez wielu wolnych klientów, szybsi użytkownicy nie są w stanie uzyskać lepszej wydajności

Dlaczego Meru Networks – Bezpieczeństwo

- Bezpieczeństwo:
  - Tunelowanie ruchu klientów bezprzewodowych od AP do kontrolera, zapewnia izolację ruchu od sieci przewodowej
  - Wbudowany w kontroler Firewall pozwala limitować pasmo lub ograniczać dostęp do określonych usług
  - Funkcje detekcji i zakłócania obcych punktów dostępowych

Meru Networks	Tradycyjne sieci
Dzięki tunelowaniu ruchu zarządzającego oraz ruchu klientów bezprzewodowych między AP a kontrolerem, jest on praktycznie odizolowany od sieci lokalnej dopóki nie zostanie przepuszczony przez Firewall kontrolera i wprowadzony np. do odpowiedniego VLANu	Tradycyjne sieci często nie korzystają z tunelowania ruchu, tylko zostawiają go „samemu sobie” w miejscu gdzie podłączony jest punkt dostępowy, lub nawet jeżeli go tunelują nie posiadają Firewalla który mógłby ten ruch sprawdzać
Wbudowany w kontroler Firewall pozwala ograniczać pasmo dla poszczególnych sieci lub użytkowników, blokować dostęp użytkowników do określonych adresów IP lub usług, a także znakować ruch za pomocą tagów QoS tak aby później mógł on być odpowiednio przesłany przez sieć przewodową	Inni producenci często rezygnują z Firewalla, pozostawiając ruch bezprzewodowy bez nadzoru, wpływa to zmniejszenie bezpieczeństwa całej sieci
Kontroler i AP posiadają wbudowane mechanizmy pozwalające na wykrywanie „obcych” AP oraz „obcych” stacji bezprzewodowych, a także na zakłócanie „obcych” punktów dostępowych w razie wystąpienia zagrożenia	Zwykłe rozwiązania często nie posiadają w ogóle mechanizmów wykrywania i zakłócania obcych sieci, lub posiadają jedynie podstawowy mechanizm wykrywania „obcych” AP bez możliwości ich zakłócania w razie wystąpienia zagrożenia

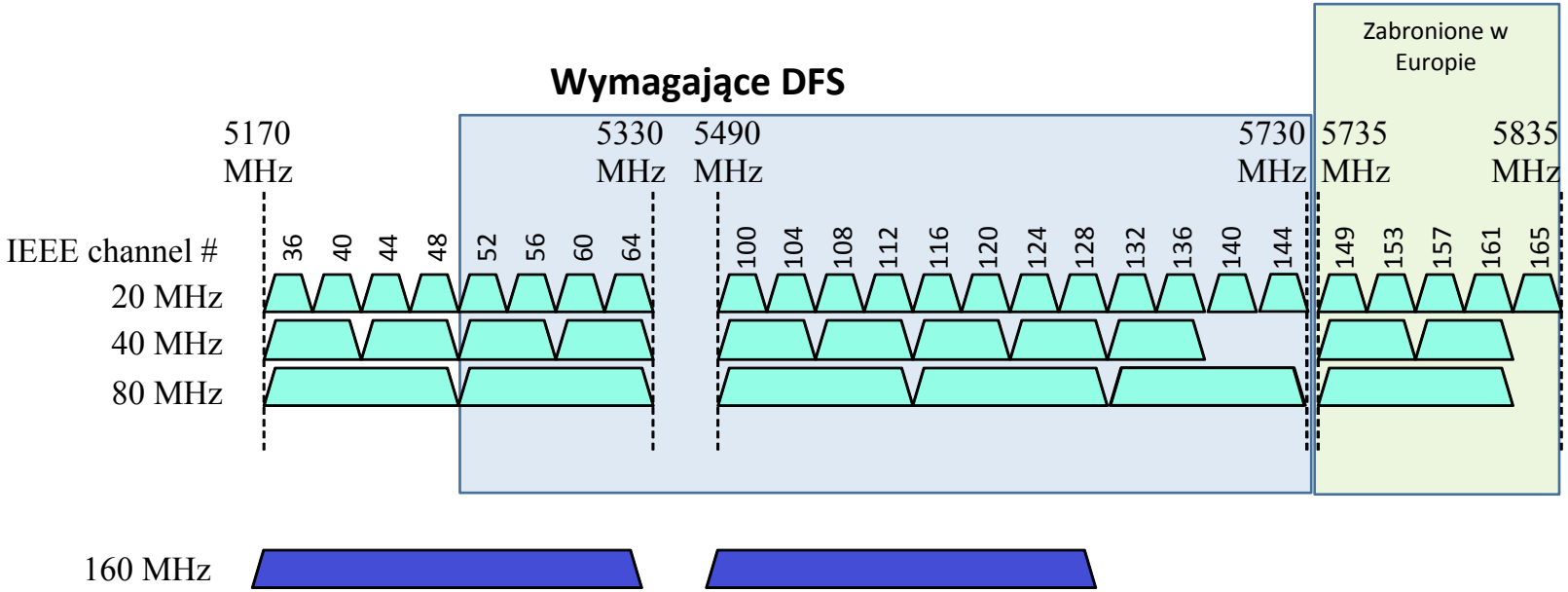
Dlaczego Meru Networks – 802.11ac(1)

- Przygotowane na nowy standard:
  - Dzięki architekturze SCA(jeden kanał), Meru będzie w stanie wykorzystać w pełni możliwości 802.11ac, ponieważ wymaga tylko 1 kanału o szerokości 80 MHz aby pokryć większy obszar
  - Sieci tradycyjne będą potrzebowały 3 kanałów o szerokości 80 MHz w paśmie 5 GHz co będzie wymagało zastosowania kanałów przeznaczonych na zewnątrz budynków z wymogiem DFS, a w dalszym rozwoju 3 kanałów o szerokości 160 MHz, czego w paśmie 5 GHz w Europie wydzielić się nie da

	20MHz	40MHz	80MHz	160MHz
1 strumień	**86.7**	**200**	**433.3**	866.7
2 strumienie	**173.3**	**400**	**866.7**	1733.3
3 strumienie	**288.9**	**600**	**1300**	2340
4 strumienie	346.7	800	1733.3	3466.7
5 strumieni	433.3	1000	2166.7	4333.3
6 strumieni	577.8	1200	2340	5200
7 strumieni	606.7	1400	3033.3	4095
8 strumieni	693.3	1600	3466.7	6933.3

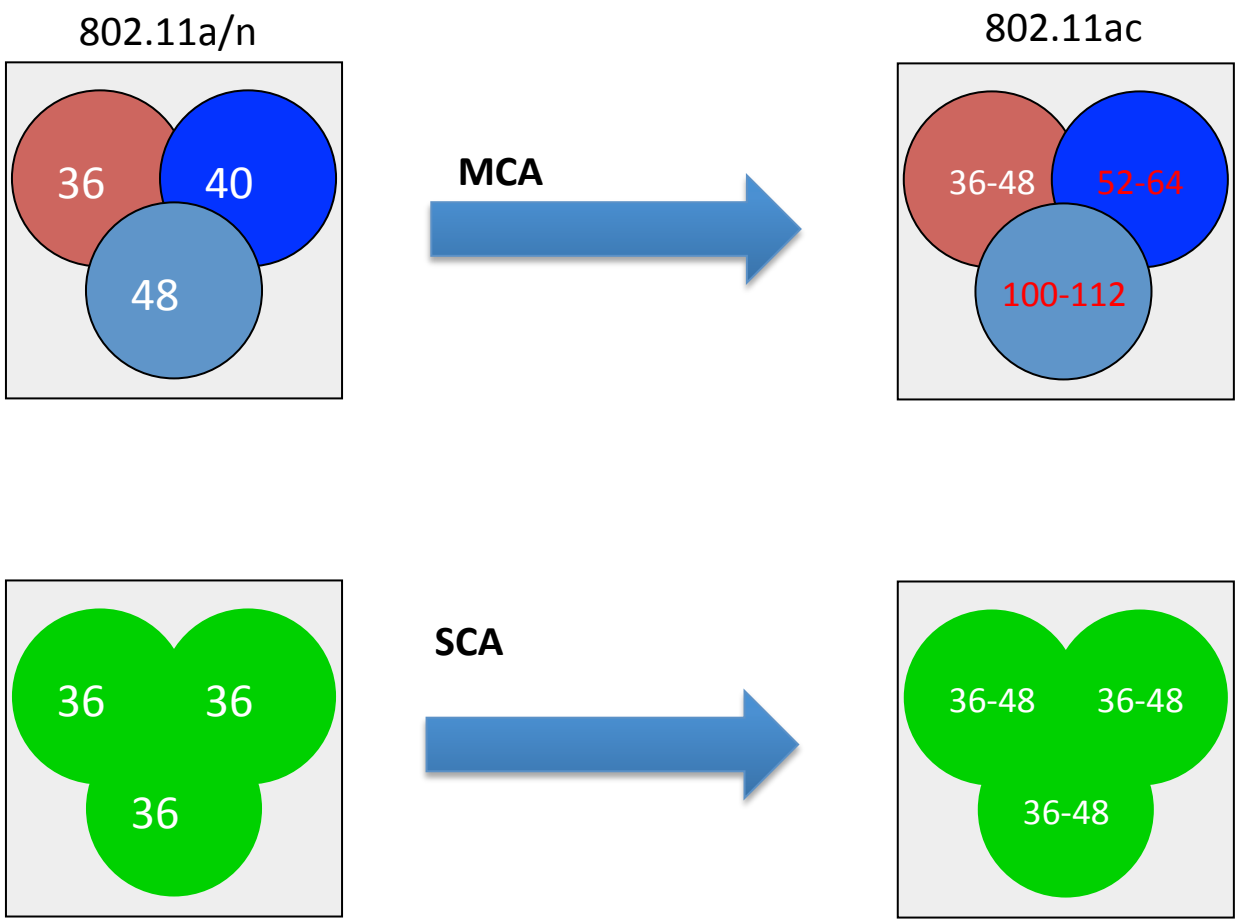
Przewidywane w pierwszej generacji chipsetu

Dlaczego Meru Networks – 802.11ac(2)



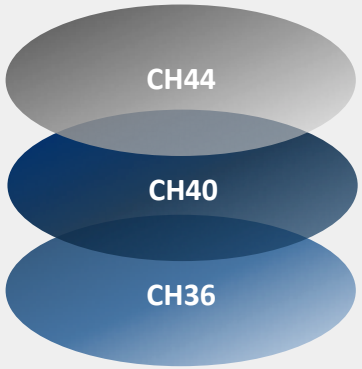
	Wymagany DFS		Nie wymagany DFS	
Szerokość kanału	US	Europa	US	Europa
40 MHz	8	9	4	2
80 MHz	4	5	2	1
160 MHz	1	2		

Dlaczego Meru Networks – 802.11ac(3)



Przyszłość w architekturze jednokanałowej

Architektura wielokanałowa wymaga wielu kanałów żeby w ogóle móc funkcjonować



"80 MHz channels – twice the capacity of 40 MHz, but not recommended for multi-AP deployments"

"Deploy with 40 MHz to minimize co-channel interference"

"In order to reduce co-channel interference it is recommended that you derive your channel plan using non-overlapping 20 MHz or 40 MHz channels instead..."

Kanał 80 MHz 1.3 Gb/s → **Kanał 40 MHz 600 Mb/s** = **Ponad 50% Redukcja Przepustowości**