ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра Комп'ютерних наук

Пояснювальна записка

до бакалаврської роботи
на ступінь вищої освіти бакалавр
на тему: «**ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ОПТИМІЗАЦІЇ РАДІОЧАСТОТНОГО РЕСУРСУ НА БАЗІ ПРОГРАМНО-АПАРАТНОГО КОМПЛЕКСУ ARUBA**».

Виконав: студент 4 курсу, групи КНД–42
спеціальності 122 Компютерні науки
(шифр і назва спеціальності)
Константінов І.О.
(прізвище та ініціали)

Керівник Гніденко М.П
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

Київ – 2020

ВСТУП

Робоче середовище для підприємств, які переходить на цифрові робочі місця, де дуже стрімко зростає щільність пристроїв та зростаючі потреби в даних визначаються BYOD, IoT, мобільними додатками та уніфікованими комунікаціями. Щоб забезпечити постійно працюючу мережу з бажаною продуктивністю та зручністю користування, підприємства повинні забезпечити безпроводову локальну мережу з передовими технологіями управління радіо, які можуть оптимізувати її поведінку у радіочастотному середовищі для підвищення ефективності та продуктивності мережі.

Радіочастотний ресурс (Radio frequency - RF) - це обмежений та спільний ресурс і для забезпечення оптимального забезпечення користувачів доступом до безпроводової мережі необхідно контролювати якомога більше його факторів. Щоб оптимізувати досвід для користувачів, стабільність мережі вимагає нового рівня інтелекту, щоб швидко адаптуватися до мінливих радіочастотних умов у мережі - наприклад, більшої щільності мережевих пристроїв, інтерференції суміжного каналу (CCI), розривів у покритті та роумінгу.

Aruba Adaptive Radio Management (ARM), вбудований в ArubaOS, динамічно налаштовує радіочастотне середовище, щоб забезпечити найкраще радіозв'язок та QoS, одночасно пом'якшуючи перешкоди спільного каналу та сусіднього каналу.

Технологія адаптивного радіозв'язку (ARM), яка контролює якість каналів безпроводових мереж Aruba, підвищує надійність та продуктивність, використовуючи засоби керування на основі інфраструктури для підвищення загальної продуктивності мережі для розгортання безпроводового зв'язку. Адаптивне радіочастотне сканування на всіх точках доступу Aruba гарантує, що контролер обізнаний про миттєву інтерференцію та індекси покриття.

В той же час, робота системи ARM не є повністю автоматизованою. Для забезпечення найбільшої ефективності функціонування безпроводової мережі необхідно здійснити оптимізацію використання радіочастотного ресурсу. Це вимагає дослідження ефективності роботи різних режимів Aruba Adaptive Radio Management (ARM) в умовах сканування і моніторингу ефіру та спектру, аналізу впливу інтерференції на ефективність безпроводової мережі, застосування AirWave Management Platform (AMP) для управління радіочастотним ресурсом та алгоритму роботи автоматичної адаптації радіочастотного середовища.

1 УПРАВЛІННЯ ТА ОПТИМІЗАЦІЯ РАДІОЧАСТОТНОГО РЕСУРСУ БЕЗПРОВОДОВИХ МЕРЕЖ ARUBA

1.1. Компоненти управління радіочастотним ресурсом безпроводових мереж Aruba

Інтерференція в мережі WLAN 802.11 є як неминучим, так і непередбачуваним явищем. Це залежить від пристрою (мікрохвильова піч, безпроводовий телефон), способу використання (різниця у часі) та місця розташування (місцеві норми викидів, конструкція). Цим потрібно керувати, щоб забезпечити надійну роботу мережі Wi-Fi. Це вимагає інтегрованого набору функцій, який постійно контролює радіочастотне середовище на предмет низької якості каналу, оптимізує радіочастотну систему без ручного втручання та забезпечує видимість у повітрі за допомогою інтуїтивних засобів усунення несправностей.

Технологія адаптивного радіозв'язку (Adaptive Radio Management - ARM), яка контролює якість каналів безпроводових мереж Aruba, підвищує надійність та продуктивність, використовуючи засоби керування на основі інфраструктури для підвищення загальної продуктивності мережі для розгортання безпроводового зв'язку. Адаптивне радіочастотне сканування на всіх точках доступу Aruba гарантує, що контролер обізнаний про миттєву інтерференцію та індекси покриття. Індекси включають робочий цикл без Wi-Fi, мінімальний рівень шуму, повторні спроби в ефірі та помилки PHY. ARM використовує цей інтелект для вжиття необхідних дій для відновлення ефективності роботи в зоні ураження. Крім того, такі функції управління інфраструктурою, як діапазонне управління (band steering), балансування навантаження спектра та справедливість ефірного часу, підвищують загальну продуктивність мережі, рівномірно балансуючи клієнтів. Отриманий користувальницький досвід - це надійна високопродуктивна мережа, яка робить спільний носій менш схожим на хаб і більше нагадує комутатор.

У більшості розгортань WLAN основне джерело будь-якого погіршення продуктивності починається на рівні 1, тобто на рівні радіочастотного спектру або на фізичному рівні. Aruba пропонує інтегрований аналіз спектру, який додає рівень видимості до безпроводових локальних мереж 802.11. Прозорість у радіочастотному діапазоні дозволяє мережевому інженеру бачити, що

відбувається в ефірі і є ключовою вимогою для усунення таких проблем. Спектральний аналіз може класифікувати та ідентифікувати джерела інтерференції, що не відповідають стандарту 802.11, забезпечуючи аналіз у режимі реального часу в точці, де виникає проблема. Найкраще використовувати його як інтегрований в інфраструктуру WLAN, оскільки ручні інструменти корисні лише тоді, коли IT-персонал знаходиться на місці та інтерференції присутня - малоймовірна комбінація на розподілених підприємствах. Рішенням проблеми є набір інтегрованих інструментів, які забезпечують прозорість з боку існуючої інфраструктури. Як показано на Рисунку 1.1, набір продуктів Aruba контролерів мобільності та точок доступу працює разом для сканування та звітування щодо джерел інтерференції.

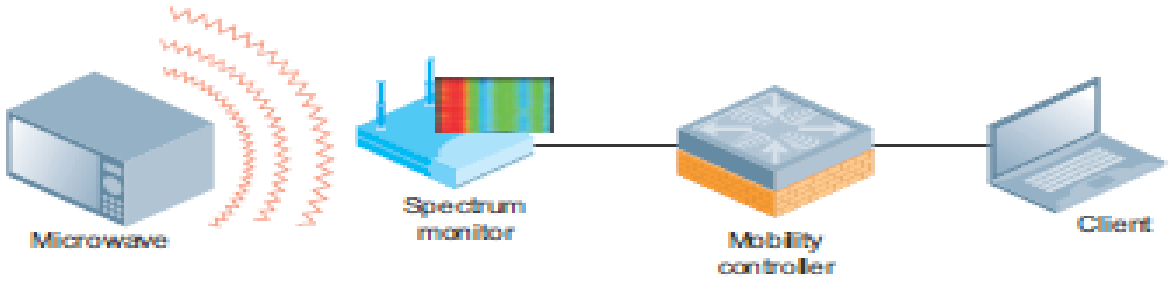

Рисунок 1.1 Аналіз спектру за допомогою контролерів мобільності та точки доступу Aruba

Aruba поєднує можливості функціональних можливостей апаратного аналізу спектра з програмним забезпеченням ArubaOS, щоб забезпечити виявлення та класифікацію джерел перешкод як 802.11, так і не 802.11. Точки доступу сканують навколишнє середовище та передають інформацію до контролера мобільності Aruba. Контролер оснащений повністю інтегрованою панеллю аналізу спектра, показаною на Рисунку 1.2. Ця панель забезпечує інформацію про візуалізацію радіочастот.

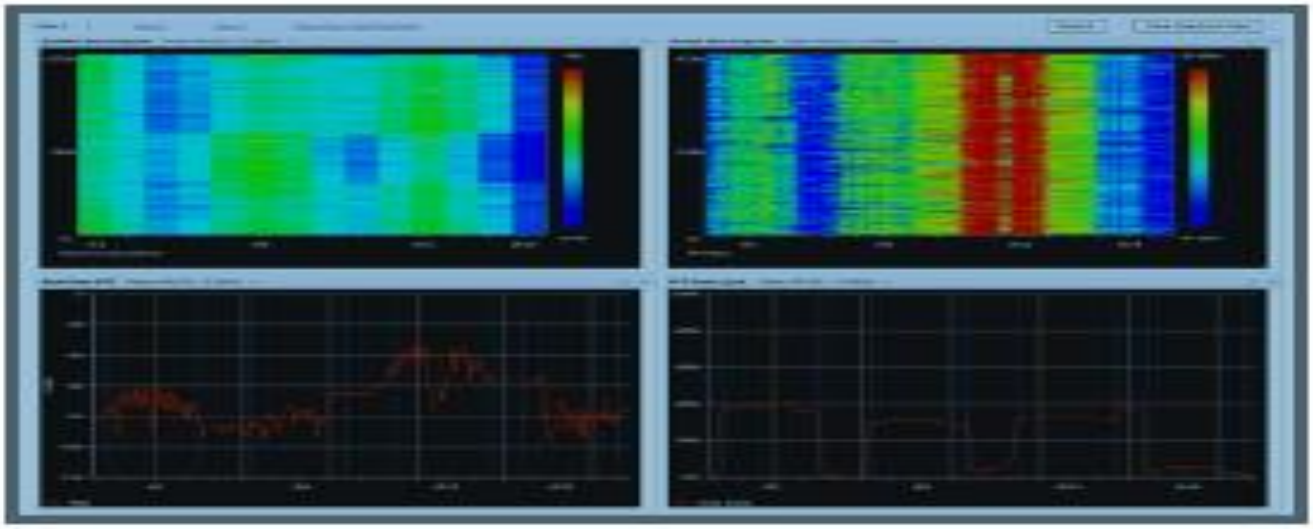

Рисунок 1.2 Інформаційна панель аналізу спектра Контролера мобільності

Як показано на Рисунку 1.3 нижче, платформа управління AirWave (AMP) - це унікальне рішення для управління Aruba, яке інтегрує конфігурацію, управління та усунення несправностей як для проводових, так і для безпроводових пристроїв для багатопрофільної мережі в одному пристрої. Вона пропонує повну інтеграцію зі статистикою ARM та інтегрується з інформаційною панеллю аналізу спектру, розміщеною в Aruba Mobility Controller для візуалізації. Окрім того, попередження RF (Radio-frequency) в режимі реального часу інформують адміністратора, коли виникає проблема, тенденційна та історична інформація про RF дозволяє проводити судово-медичний аналіз, а звіти про стан RF допомагають у проактивному плануванні.

Рисунок 1.3 Платформа управління AirWave

Наступні компоненти складають інтегроване рішення Aruba для забезпечення прозорості радіочастотного ресурсу:

багатоцільові точки доступу;

контролер мобільності Aruba з ліцензією RFProtect ™;

платформа управління AirWave (AMP).

Багатоцільові точки доступу. Точки доступу Aruba 802.11n засновані на технології Atheros XSpan. Набір мікросхем Wi-Fi від Atheros був розроблений з нуля з інтегрованими можливостями аналізу спектра високої чіткості як однією з основних цілей. Завдяки спеціально побудованому процесору та виділеному TPM (Trusted Platform Module), платформи AP Aruba 802.11n здатні виконувати кілька операцій без шкоди для безпеки та без додаткових витрат. Існує три режими роботи для точки доступу Aruba, це гібридний режим, режим моніторингу ефіру (Air Monitor - AM) та режим моніторингу спектру (Spectrum Monitor - SM) відповідно. Давайте розглянемо різні режими роботи точки доступу Aruba більш докладно.

Режим точки доступу (Access Point - AP). Коли точка доступу працює в режимі точки доступу, вона буде обслуговувати клієнтів і періодично виходити за межі каналу, щоб сканувати середовище радіочастот для оцінки навколишнього радіочастотного покриття. У цьому режимі він також може збирати події IDS (Intrusion Detection System), виконувати виявлення зловмисних впливів та їх стримування. Хоча точка доступу не виконує сканування спектру в цьому режимі, вона все одно буде контролювати показники інтерференції та покриття у навколишньому середовищі. Коли рівень інтерференції перетинає певний поріг, технологія адаптивного радіозв'язку (Adaptive Radio Management - ARM) Aruba, яка інтегрована в базовий ArubaOS, адаптує та вибирає кращий канал для підтримки надійного радіочастотного сигналу.

Гібридний режим точки доступу (Hybrid AP mode). Коли точка доступу перебуває в режимі точки доступу з увімкненим моніторингом спектру (Spectrum Monitoring), вона буде обслуговувати клієнтів і періодично виходити за межі каналу для сканування середовища на наявність подій безпеки, подібно до попереднього режиму. Крім того, вона також виконує сканування спектру на "домашньому каналі", який є каналом роботи радіо AP. Це дозволить радіостанції виявляти та класифікувати джерела інтерференції та надсилати інформацію про класифікацію до AirWave для узагальності та звітності. Більше того, він також

відображатиме діаграми спектру для візуалізації радіочастотного покриття на домашньому каналі.

Режим моніторингу ефіру (Air Monitor - AM). Коли радіо перебуває в режимі моніторингу ефіру, його функціональність обмежується безпроводовим виявленням подій IDS, виявленням зловмисників та стримуванням. Вона витрачає 100 відсотків часу на сканування каналів у налаштованому домені і не виконує ніякого сканування спектру.

Режим моніторингу спектру (Spectrum Monitor - SM). Коли точка доступу знаходиться в режимі моніторингу спектру, її головна відповідальність полягає у виконанні сканування спектра по всьому діапазоні роботи. Потім ці дані подаються до Aruba Mobility Controller та AirWave. Точки доступу також сканують для безпроводового виявлення подій IDS, виявлення зловмисників та стримування, але вони не обслуговують клієнтів у цьому режимі. Aruba має широкий асортимент точок доступу, що забезпечує велику гнучкість для клієнтів у виборі найкращого продукту, який відповідає їхнім мережевим вимогам. Усі точки доступу на Aruba мають можливість відслідковувати рівень шуму (noise aware), що означає, що вони мають можливість виявити аномалію радіочастотного покриття та вибрати кращий канал. Більше того, більшість точок доступу Aruba 11n здатні класифікувати джерела шуму.

Контролери мобільності Aruba (Aruba Mobility Controllers). Контролер мобільності Aruba є ключовим компонентом рішення, що забезпечує чіткий огляд радіочастотного покриття. Точки доступу сканують в ефірі події, пов'язані зі спектром, виявляють та класифікують інтерференцію. Вони передають цю інформацію контролеру мобільності, який узагальнює дані спектра з точок доступу з можливістю множинного аналізу спектру. Цей спектр інтелекту використовується технологією Adaptive Radio Management (ARM) для побудови таблиці сусідніх радіочастот, щоб він знав, до якого каналу рухатися, коли якість ефіру переходить певний поріг. Спектральна приладова панель, розміщена в контролері мобільності Aruba, забезпечує поглиблену візуалізацію радіочастотного покриття.

Аналізатор спектру Aruba доступний у версії ArubaOS 6.0 та новіших версіях. Це означає, що він підтримується на контролерах мобільності Aruba 600, Aruba 3000 і Aruba 6000. Функцію можна ввімкнути за допомогою ліцензії RFProtect на контролері мобільності Aruba. Кількість датчиків спектру, підтримуваних контролером, змінюється залежно від контролера і дорівнює

кількості точок доступу, які можуть підтримуватися конкретною моделлю контролера. Aruba 6000, наприклад, може підтримувати до 2048 датчиків спектру.

Необхідно звернути увагу, що інформаційна панель Spectrum (UI) інтегрована з ArubaOS WebUI, яка розміщена на контролері мобільності Aruba, до якого, як правило, можна отримати доступ зі станції управління. Aruba дозволяє підключати більше одного монітора спектру до одного екземпляра клієнтського інтерфейсу. Однак максимальна кількість одночасних SM, які можна підключити до одного клієнта інтерфейсу, буде обмежена можливостями клієнта, включаючи центральний процесор та пам'ять. Як правило, очікуйте, що даний клієнт підтримуватиме до шести SM. Крім того, кількість одночасних сеансів інтерфейсу клієнта на контролер обмежена 20.

AirWave Management Platform (AMP). AMP є ідеальною платформою управління для моніторингу всієї безпроводовоъ локальної мережі для підтримки надійної роботи та забезпечення оптимального безпроводового зв'язку для мобільних кінцевих користувачів. AMP діє як централізована система управління мережею, яка агрегує інформацію про інтерференцію в мережі. На додаток до миттєвої інформації про інтерференцію, AMP пропонує історичну інформацію, яка дозволяє налагодити та вирішити проблеми, пов'язані з продуктивністю, з більшим контекстом. Інформація варіюється від виявлення інтерференції, класифікації інтерференції, каналів, на які впливає інтерференція, робочого циклу інтерференції та позначки часу, коли інтерференція була виявлена. AMP також інтегрує відстеження місцеположення заважаючого пристрою, додаючи більше контексту до проблем продуктивності. На додаток до детальної інформації, що стосується інтерференції, AMP пропонує заздалегідь визначені, власні звіти про стан радіочастот, які виступають активним інструментом для виявлення та ізоляції проблемних пристроїв у мережі. Сповіщення в режимі реального часу повідомляють адміністраторів про проблему до того, як реєструється квиток служби підтримки, тим самим забезпечуючи більш ефективне усунення несправностей. Для детальної РЧ-візуалізації AMP має швидке посилання на приладову панель спектру, розміщену на контролері WLAN.

1.2. Налаштування точок доступу для забезпечення режиму моніторингу спектру

Розглянемо різні способи, яким чином можна зробити Aruba AP готовою до аналізу спектру, що включає спеціальний моніторинг спектру та гібридний моніторинг спектру.

Спеціальний монітор спектра налаштовується лише для моніторингу радіочастотного середовища. Ця станція може бути налаштована індивідуально, але частіше існує група AP, призначена для моніторингу спектра, яка має подібну конфігурацію.

Гібридний монітор спектру одночасно обслуговує клієнтів та надає детальний аналіз спектру. Як пояснювалося раніше, рекомендується найкраща практика визначати окрему групу для гібридних точок доступу, щоб точки доступу в мережі мали спільну конфігурацію.

Нова точка доступу, яка з’являється вперше, повинна бути забезпечена вручну у відповідній групі точок доступу. Після забезпечення, точка доступу завантажує свою конфігурацію з контролера і стає функціональною. Зазвичай це одноразовий процес, який інструктує AP до групи, до якої він належить.

Інтуїтивно зрозумілий графічний інтерфейс користувача з випадаючими параметрами вибору та яскравими кольоровими діаграмами спрощує налаштування та використання модуля аналізатора спектра на контролері мобільності Aruba. Інформаційна панель спектра розділена на дві області - рядок заголовка та область діаграми. Як видно на Рисунку 1.4 нижче, самою верхньою панеллю інформаційної панелі є рядок заголовка. Він показує три вкладки - view 1, view 2, view 3 та запис/відтворення. Кожен view дозволяє відображати 4 різні діаграми. Нижня панель відома як область діаграми, яка може відображати різні діаграми, такі як FFT (Fast Fourier transform), спектрограми, активні пристрої тощо. FFT - це механізм частотного аналізу, який спрямований на швидше перетворення дискретного сигналу у часовій області в представлення у дискретної частотної області. Aruba пропонує різноманітні вбудовані діаграми, які адміністратори можуть вибрати для кожного перегляду.

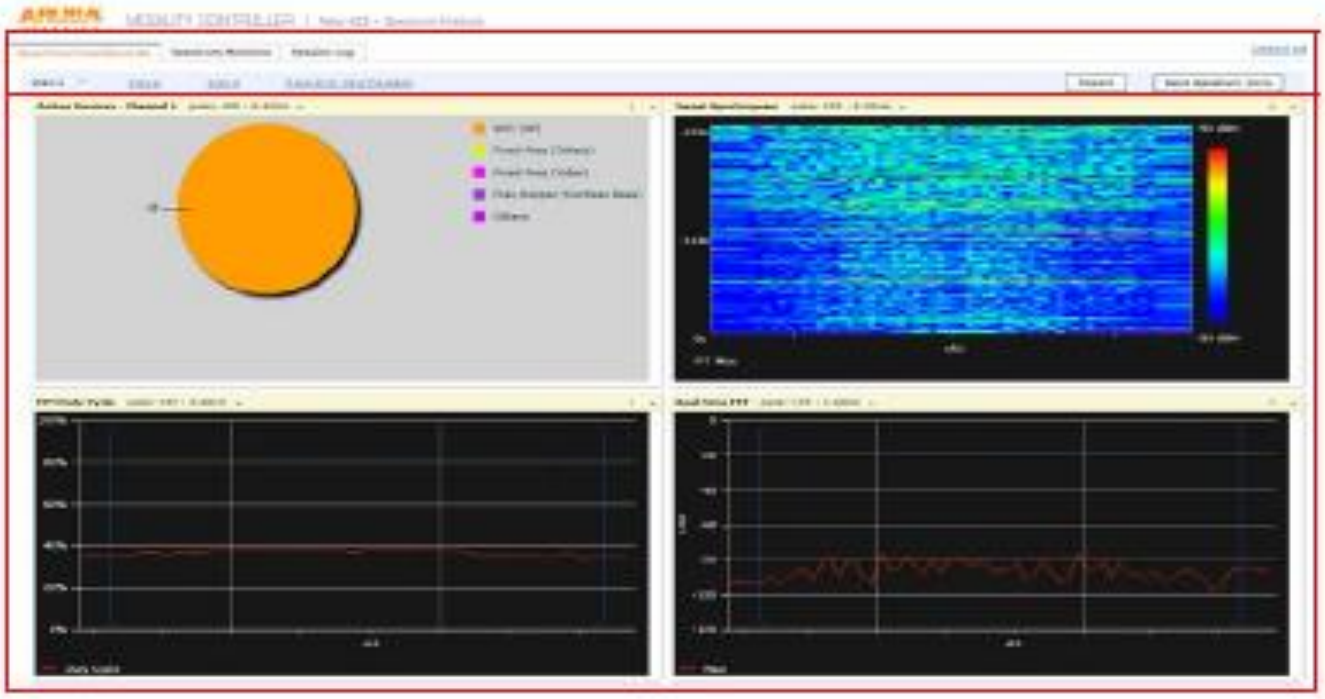

Рисунок 1.4 Інформаційна панель Spectrum

Наступні кроки детально описують процес підключення до SM та відображення графіків та діаграм середовища радіочастотного покриття.

1. Для того, щоб забезпечити візуалізацію, радіостанції AP, які необхідні для аналізу спектра, повинні бути вручну підключені, тобто необхідно вибрати радіостанції, з яких ви хочете отримати дані візуалізації.

2. Обсяг інформації, що надається інформаційною панеллю спектру, залежить від режиму роботи точки доступу. Спеціальний монітор спектра дає знімок у режимі реального часу по всьому спектру для певної радіостанції AP, як показано на Рисунку 1.5.

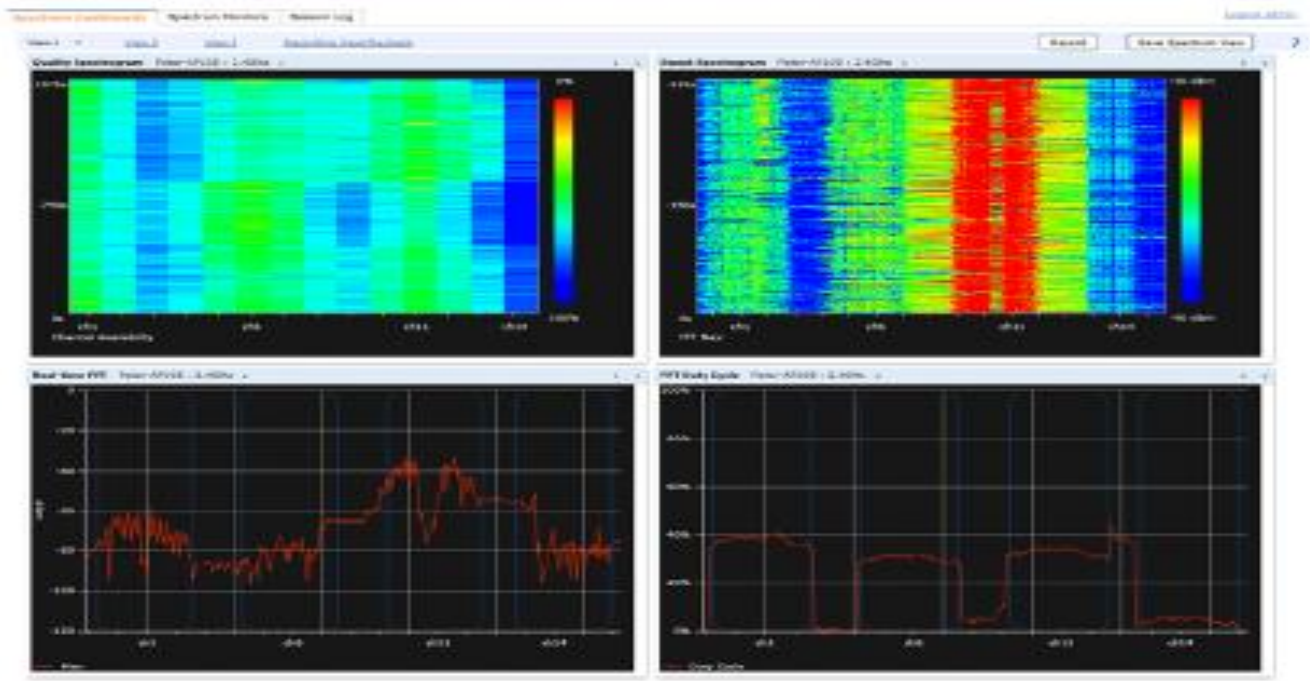

Рисунок 1.5 Інформаційна панель спектру в діапазоні 2,4 ГГц

3. Інформаційна панель спектра для гібридної точки доступу дасть знімок у реальному часі для домашнього каналу, як показано на Рисунку 1.6. У наступному розділі ми поговоримо більше про панелі спектру, діаграми та значення кожної діаграми для адміністратора WLAN.

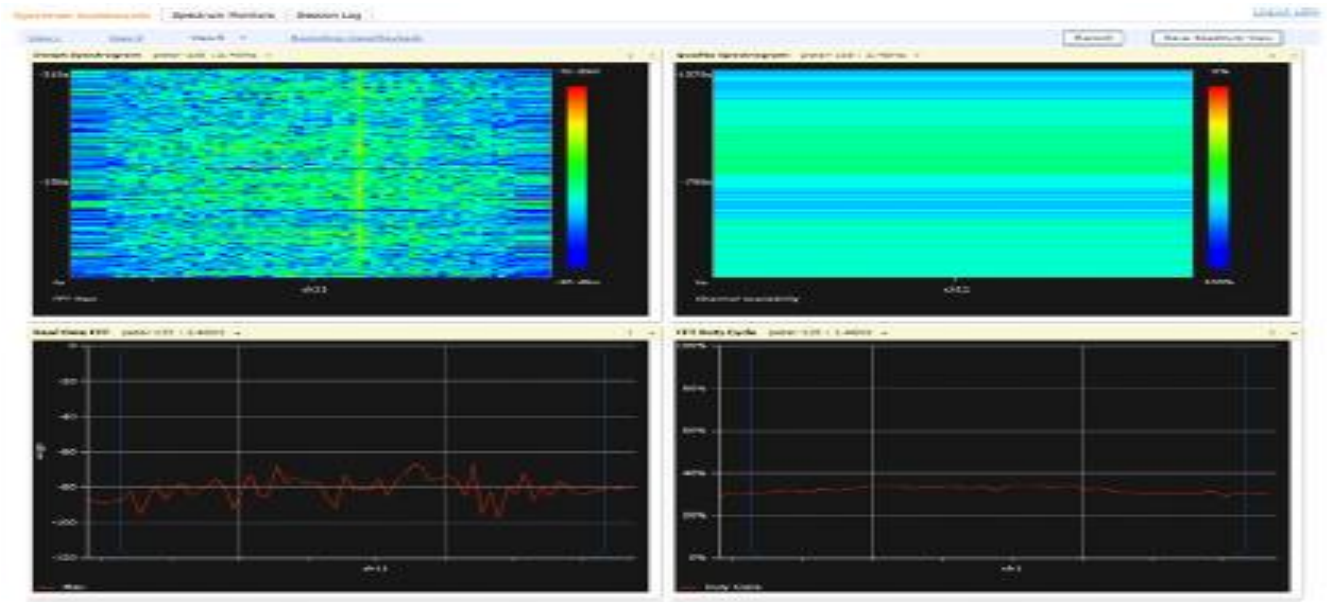

Рисунок 1.6 Інформаційна панель спектру для гібридної точки доступу на каналі 11

1.3. Застосування спектрограм для аналізу впливу інтерференції на ефективність безпроводових мереж

Кожне джерело радіочастотного випромінювання є унікальним. Випромінювання від джерела можна диференціювати на основі чотирьох факторів:

частота, на якій джерело інтерференції здійснює випромінювання;

смуга пропускання, яка зайнята випромінюванням;

потужність випромінювання на кожній з частот;

відсоток за одиницю часу, протягом якого джерело здійснює випромінювання.

Ці чотири параметри також визначають вплив, який джерело інтерференції матиме на мережу WLAN, що працює в тому ж радіочастотному просторі. Наприклад, широкосмугове джерело, що випромінює з великим робочим циклом і великою амплітудою, негативно вплине на WLAN на широкому діапазоні каналів. Вузькосмугове джерело, що випромінює з великою амплітудою, але далеко від центральної частоти, на якій працює AP, матиме менший вплив.

Ці ідентифікаційні характеристики можна дізнатись насамперед з інформації, наведеної у двох діаграмах спектру:

діаграма FFT у режимі реального часу;

діаграма робочого циклу FFT.

Діаграма FFT у режимі реального часу (Рисунок 1.7) відображає енергію, виявлену монітором спектру на кожній частотній складовій у зазначеному діапазоні. Ця діаграма відображає потужність джерела шуму.

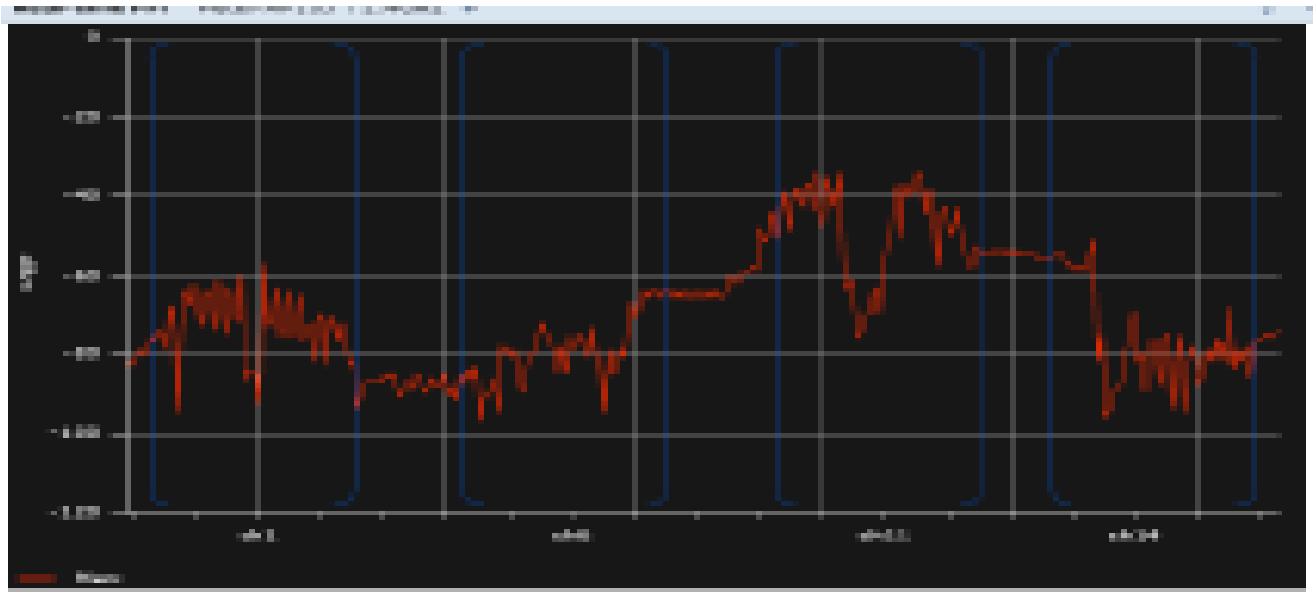

Рисунок 1.7 Діаграма FFT у режимі реального часу

Діаграма робочого циклу FFT (Рисунок 1.8) відображає відсоток часу активності інтерференції. Це дозволяє оцінити вплив інтерференції на канал.

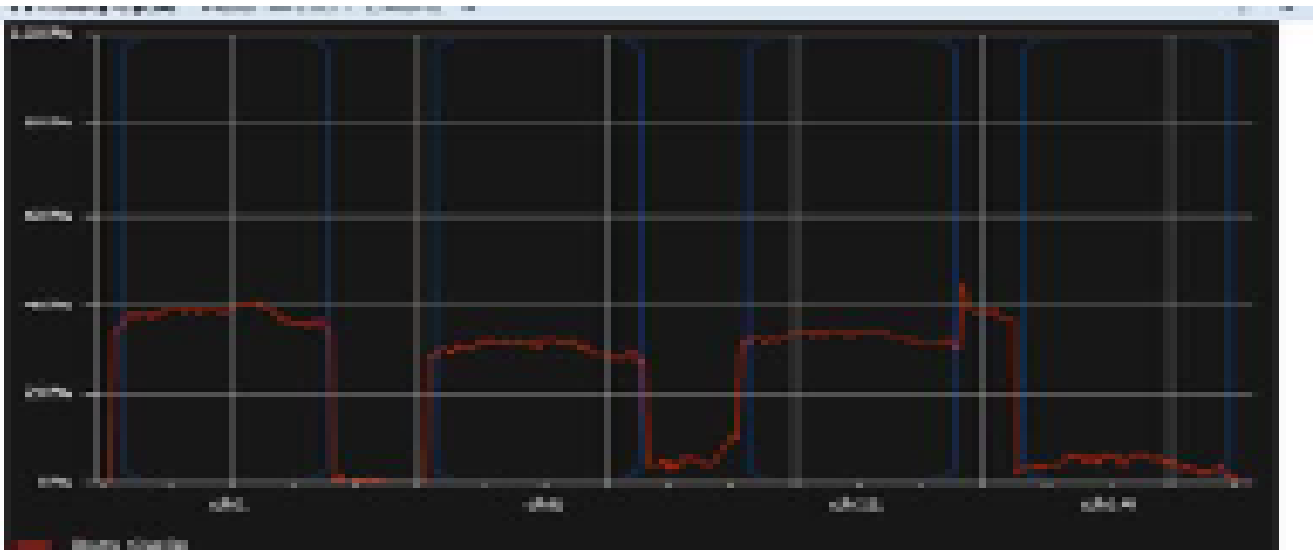

Рисунок 1.8 Діаграма робочого циклу FFT

Нижче наведено кілька прикладів, що ілюструють, як різні джерела інтерференції безпроводової локальної мережі відображатимуться на цих графіках. Виявляючи радіочастотні сігнатури, адміністратор може заздалегідь фіксувати джерела точкової інтерференції та їх вплив на довкілля.

Сігнатура AP. Точка доступу працює на каналі 1 і прослуховується монітором спектра на рівні -20 дБм (дуже близько до монітора спектра). Спектр сильно поширюється до каналу 4, а потім швидко падає (Рисунок 1.9).

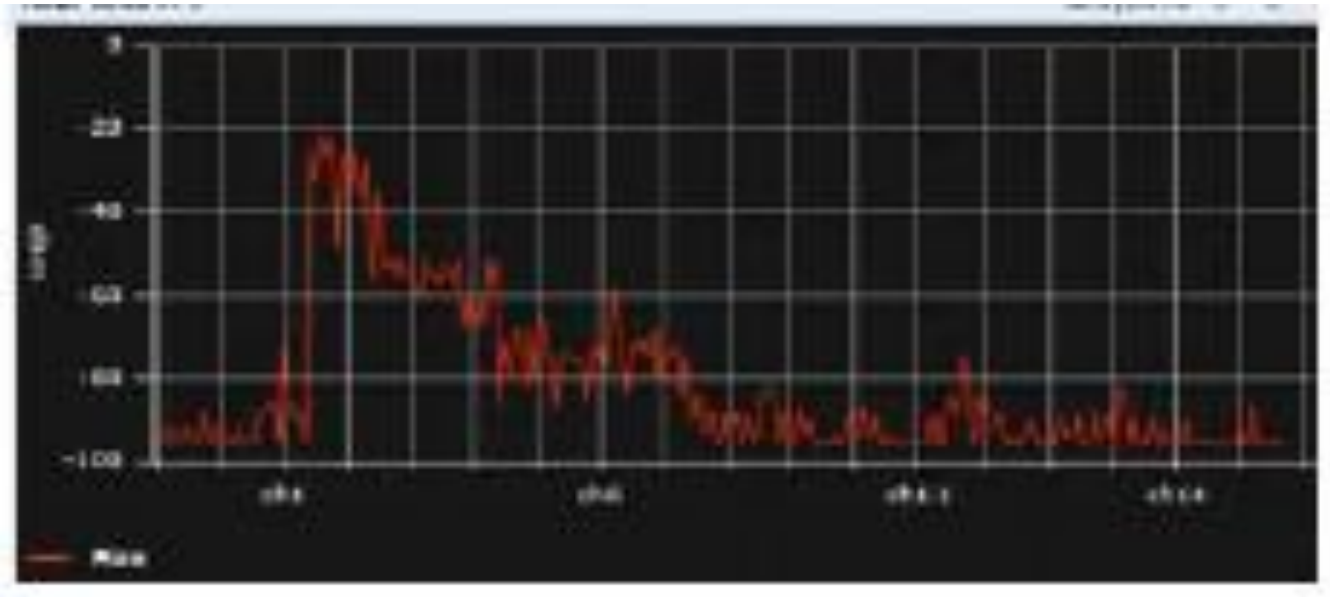

Рисунок 1.9 Сігнатура точки доступу

Сигнатура безпроводового телефону із фіксованою частотою. Пристрій працює на каналі 1, робочий цикл пристрою зазвичай становить близько 100%, що

означає, що випромінювання безперервне, а канал 1 стає непридатним для використання (Рисунок 1.10).

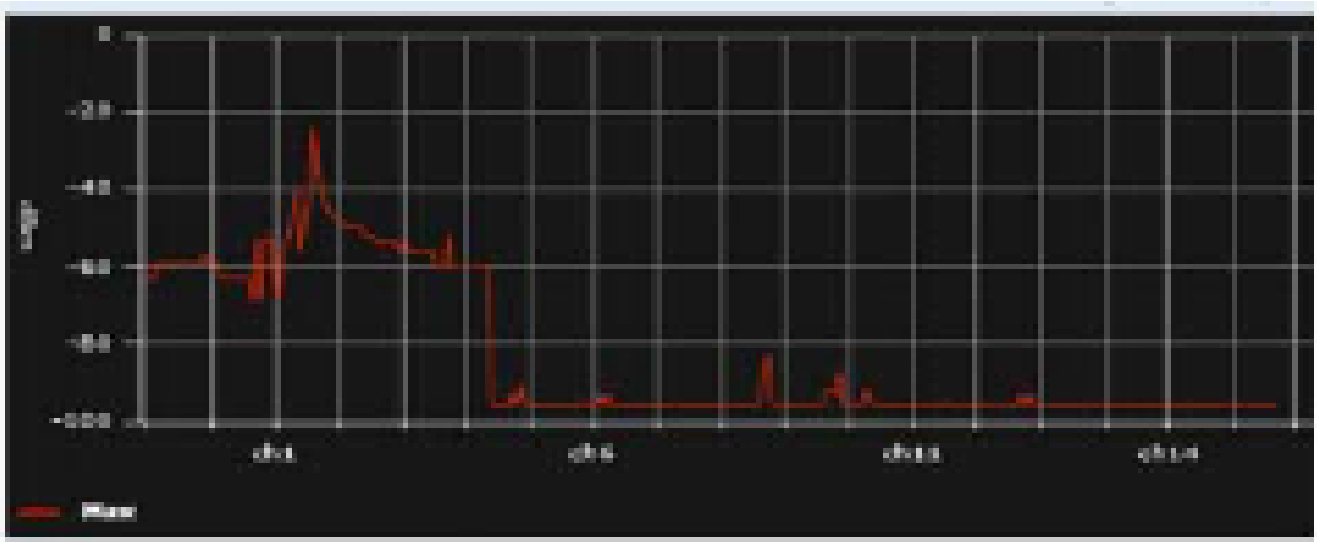

Рисунок 1.10 Сигнатура безпроводового телефону із фіксованою частотою

Сигнатура пристрою з перескоком частоти. Інтерферентор перескакує від частоти до частоти по всьому спектру 2,4 ГГц. Це є дуже руйнівними обставинами, оскільки АР буде важко знайти чистий канал (Рисунок 1.11).

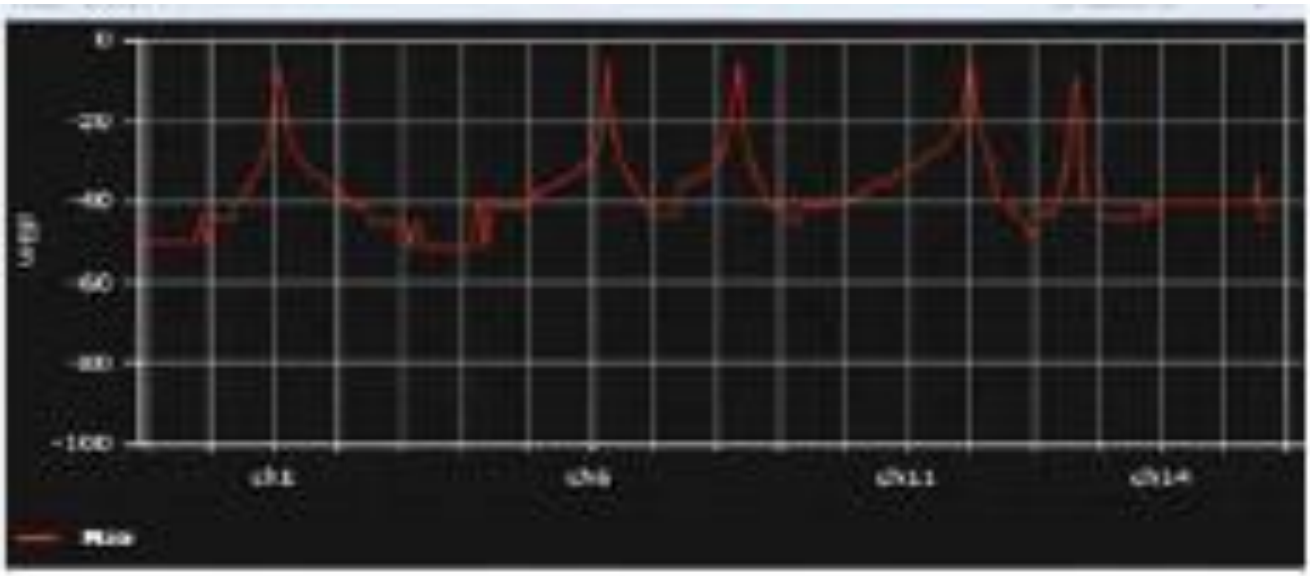

Рисунок 1.11 Сигнатура пристрою з перескоком частоти

Swept спектрограма. Ця діаграма являє собою кольоровий вигляд FFT в режимі реального часу, який вказує на силу перешкод. Синій до зеленого - це добре чи прийнятно, тоді як жовтий, оранжевий та червоний призводять до поганої роботи WLAN (Рисунок 1.12).

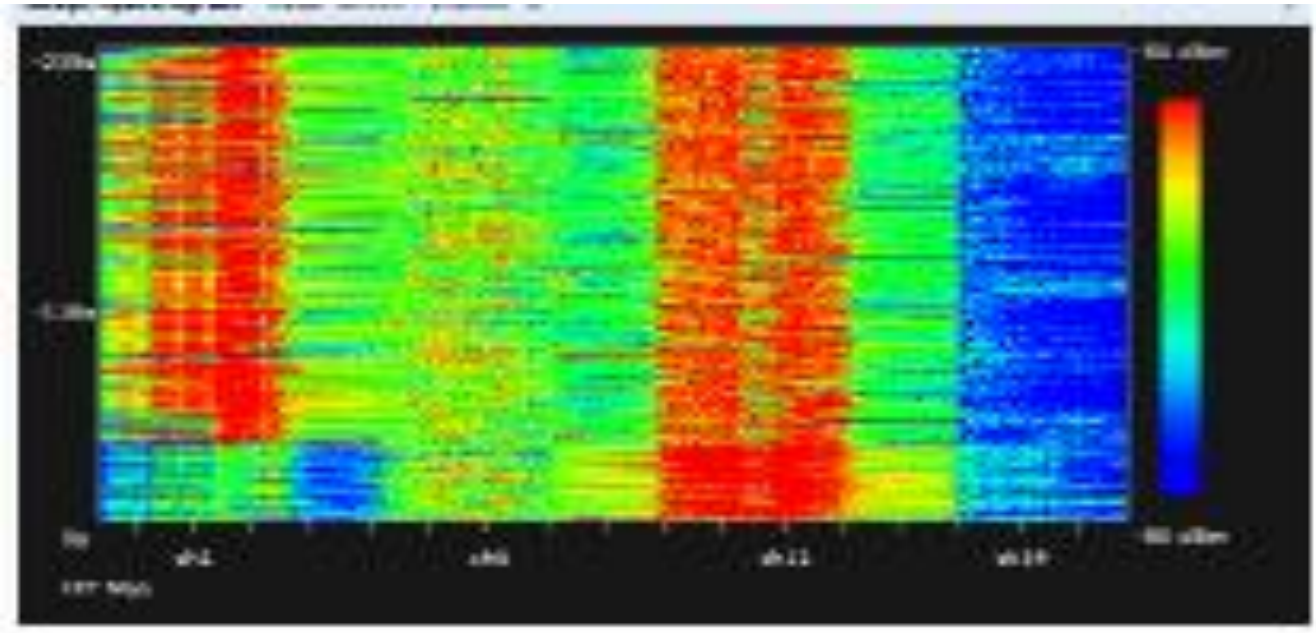

Рисунок 1.12 Swept спектрограма

Спектрограма якості. Це кольорова діаграма, яка показує якість каналу протягом певного періоду часу. Синій або зелений вказує на хорошу продуктивність, тоді як жовтий, оранжевий та червоний призведуть до неоптимальної продуктивності WLAN (Рисунок 1.13).

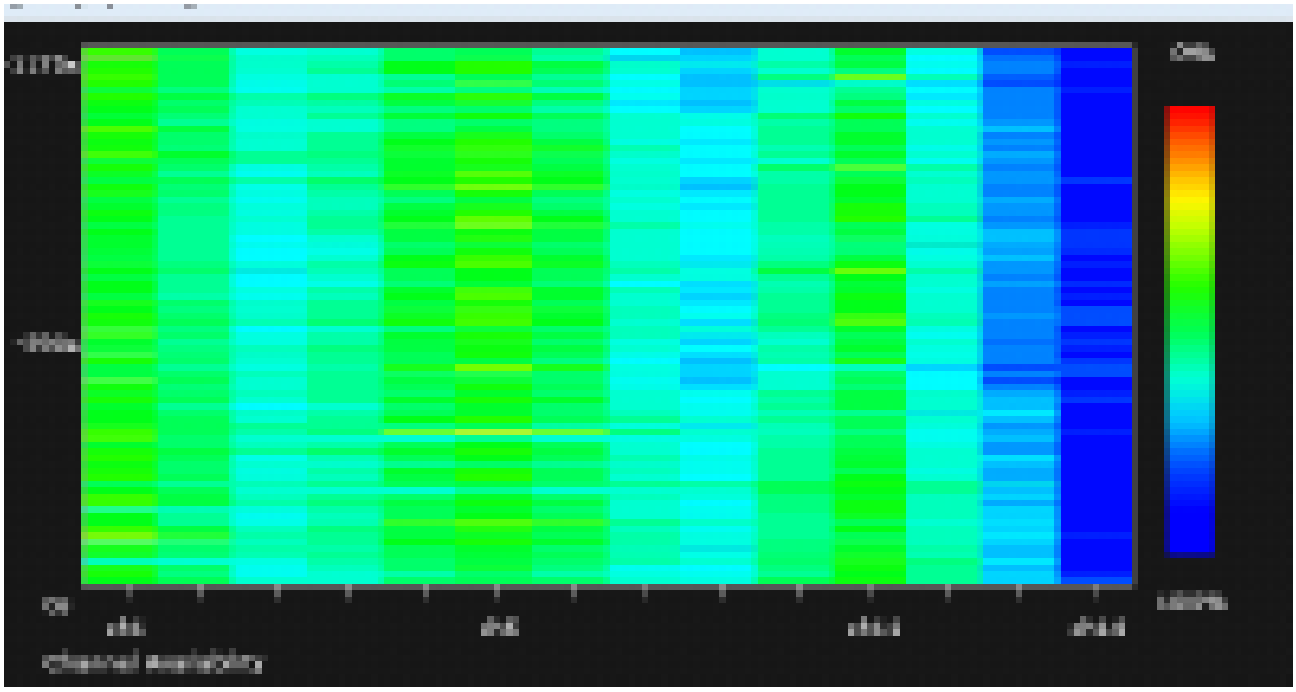

Рисунок 1.13 Спектрограма якості

1.4. Застосування AirWave Management Platform (AMP) для управління радіочастотним ресурсом безпроводових мереж Aruba

AMP надає інформацію в інтуїтивно зрозумілому графічному форматі, який допомагає адміністратору зрозуміти RF середовище та вжити необхідних коригувальних заходів. Необхідно знайти потрібну точку доступу в мережі, ввівши її назву в рядку пошуку AirWave. Коли AirWave знайде точку, що цікавить, виберіть точку, щоб перейти до сторінки моніторингу точки доступу. Виберіть будь-яку з радіостанцій на сторінці моніторингу точки доступу, щоб перейти на сторінку статистики окремих радіостанцій.

Розділ підсумків випусків містить інформацію, що стосується мінімального рівня шуму, кількості користувачів, пристроїв, що заважають, використання каналів, пропускної здатності, помилок MAC та PHY. Цей розділ повідомляє адміністратора про те, що проблема є, він допомагає визначити, в чому проблема, та виділяє причину проблеми. За замовчуванням пороги спрацьовування випуску такі:

Issue	Triggering Threshold
High Noise	-80
High number of Users	15
High Channel Utilization	75%
High Bandwidth	75% of max
Interfering Devices Detected	Detected within the last 5 minutes
High MAC/PHY Errors	1000 frames/sec

Графіки часових рядів для радіо відображаються через подвійний інтерфейс із вкладками, щоб показати зміни, які записані через різні інтервали часу опитування. Це графіки в режимі реального часу, які надають знімок радіочастотного середовища з історичною інформацією до року включно. Деякі з цих відповідних графіків, пов'язаних з радіочастотним ресурсом, - це канал, шум і потужність, лічильники 802.11 та використання каналів. Крім того, ці графіки також надають інформацію про користувача та пропускну здатність, пов'язану з певним радіо. Типовий графік радіостатистики на AirWave показаний нижче на Рисунку 1.14.

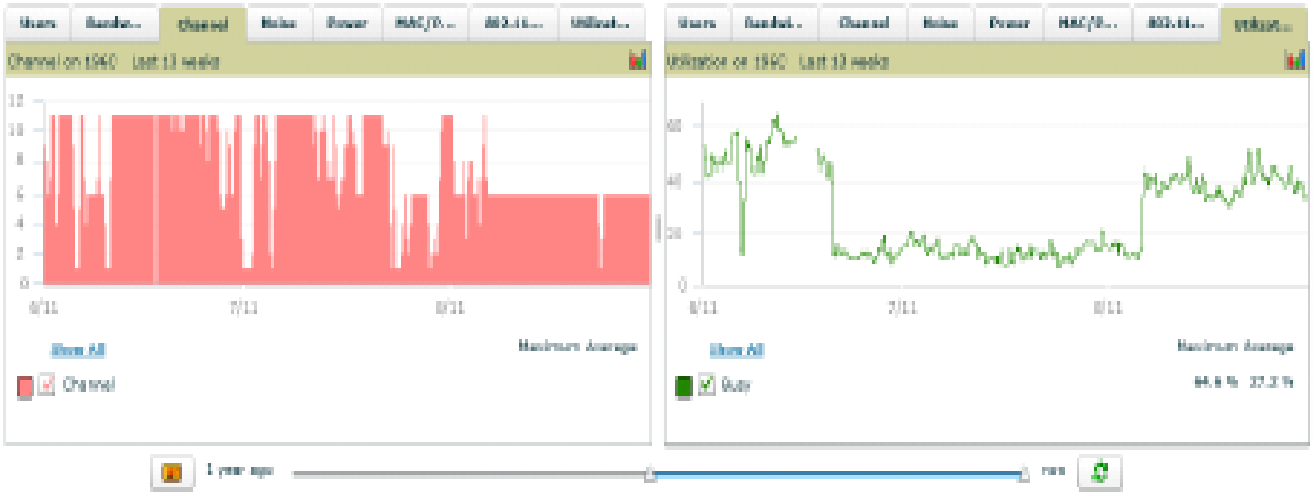

Рисунок 1.14 Графіки радіостатистики з історичними даними

Для точок доступу Aruba, що працюють в гібридному режимі, або в режимі спектра, ті самі пристрої, що не належать до 802.11, визначені в розділі підсумків проблем, класифікуються в таблиці виявлених пристроїв інтерференції разом із міткою часу останнього виявлення, початковим і кінцевим каналами інтерференції, відношення сигнал/шум (SNR) та робочий цикл інтерференції, як показано на Рисунку 1.15.

1-7 of 7 Interfering Devices Page 1 of 1 Choose Columns CSV Export

Device Type	Last Seen	Start Channel	End Channel	SNR	Duty Cycle
Cordless Base Freq Hopper	1/14/2011 3:31 PM	1	14	69	5
XBox Freq Hopper	1/14/2011 3:17 PM	1	14	63	5
Cordless Phone Freq Hopper	1/14/2011 2:10 PM	1	14	80	5
Generic Freq Hopper	1/14/2011 3:52 PM	1	14	73	5
Video Device Fixed Freq	1/14/2011 9:25 AM	10	13	72	99

Рисунок 1.15 Таблиця виявлених пристроїв інтерференції

На додаток до статистики радіочастот, яку надає AMP, він також пропонує візуалізацію радіочастот, надаючи швидке посилання на панель аналізу спектра для поглибленого аналізу джерел інтерференції, що не стосуються 802.11. Це запускає інформаційну панель спектра без необхідності в додатковому програмному або апаратному компоненті, тим самим полегшуючи пошук несправностей для адміністратора WLAN.

Щоб надати більше контексту для проблем, що виникають у безпроводовій мережі, потрібно знати, де знаходяться користувачі та пристрої і потрібно стежити за радіочастотним середовищем у цих областях. Візуальний RF (VRF) модуль в AMP забезпечує зображення в реальному часі радіосередовища у

прямому ефірі безпроводової мережі. Для забезпечення видимості в радіочастотному режимі AMP використовує сучасну технологію відбитків пальців і порівнює джерела інтерференції, повідомлених з декількох точок доступу, для триангуляції місця розташування інтерференції. Після того, як інтерферентні пристрої знайдені, це дозволяє Visual RF відображати місце розташування інтерференції. Відстеження місцезнаходження інтегровано в систему управління мережею, не вимагає жодної додаткової конфігурації, апаратних приладів або відповідних ліцензій.

AMP розробила звіти для однозначного відстеження радіочастотного середовища в певному розгортанні та виявлення проблем. AMP пропонує як спеціальні, так і вбудовані звіти про стан радіочастот для зручності використання. Вбудований звіт про стан радіочастот відслідковує найпопулярніші радіостанції точки доступу за шумом, помилками MAC/PHY, зміною каналів, зміною потужності передачі, зміною режиму та заважаючими пристроями. Крім того, він допомагає визначити найбільш проблемні пристрої у мережі та перелічує 10 найкращих пристроїв за типом проблеми. Спеціальні звіти про технічний стан можна визначити за кількома ключовими параметрами, які цікавлять адміністратора.

Розглянемо приклад безпроводової мережі із застосуванням AirWave Management Platform (AMP) для управління радіочастотним ресурсом.

У мережі маємо 3 гібридні точки тоступу AP-135 з іменами 135-1, 135-2 та 135-3. Оскільки це гібридні точки доступу, вони будуть обслуговувати клієнтів та виконувати аналіз спектру одночасно. Ці точки доступу мають кілька клієнтів, пов’язаних із ними. Усі точки доступу закінчуються на контролері мобільності Aruba 3600. Точками доступу та контролером WLAN керує платформа управління AirWave.

За наявності джерела шуму з великим робочим циклом, такого як відеоміст, продуктивність клієнта страждає. Як безпроводова локальна мережа Aruba допомагає виявляти проблему та усувати її в режимі реального часу?

1. На AMP було налаштовано тригер використання каналу, який генерує повідомлення електронною поштою адміністратору WLAN у разі поганої якості ефіру.

2. У цьому сценарії AMP було налаштовано на створення сповіщення електронною поштою про складну умову відповідності. Умова полягає в наступному - виявлена інтерференція, яка не пов'язана з 802.11, повинна

становити більше 5% від доступного каналу, використання каналу більше 5%, а джерело інтерференції спостерігається мінімум протягом 1 хвилини.

Джерелом шуму, використаним у цьому прикладі, є широкосмугове джерело шуму з фіксованою частотою. Відеомост - це джерело шуму з великим робочим циклом (~ 90%), яке працює в діапазоні частот у своєму діапазоні (2,4 або 5 ГГц). Якість ефіру в районі радіопокриття погіршиться, що негативно вплине на взаємодію з користувачем.

Важливо зазначити, що Adaptive Radio Management (ARM) виявить низьку якість каналу за наявності відеомоста та динамічно вибире кращий канал. Однак відеоміст є широкосмуговим джерелом шуму і, отже, впливає на всі корисні канали в діапазоні 2,4 ГГц.

Гібридні AP-135 постійно сканують джерела шуму, що не належать до стандарту 802.11, та інші заходи безпроводової безпеки в домашньому каналі, а також регулярно виконують сканування поза каналами. Точка доступу може виявити низький рівень шуму та подати цю радіочастотну інформацію до контролера мобільності Aruba. AP також виявляє та класифікує джерело шуму. Контролер може взяти цю інформацію з точки доступу і відобразити її у вигляді діаграм для візуалізації. Контролер WLAN передає цю інформацію в систему управління AMP. Коли умови використання відповідного каналу, налаштовані на AMP, виконуються, він автоматично генерує повідомлення електронною поштою адміністратору WLAN. У таблиці нижче показана інформація, яку адміністратор отримує як частину сповіщення.

Value	Information on the alert
What is the matching condition for the trigger?	Interference, Channel Utilization
What is the severity level of the trigger?	Critical
What are the affected devices?	135-1 and 135-3
What is the affected radio?	802.11bgn radio on both the APs
Where are they located?	Location information floor plan level visualization
Link to More detailed info	Link to the AP monitoring page on AMP that offers detailed statistics

Необхідно вибрати гіперпосилання, надане для AP-135-1, у сповіщенні. Відкриється сторінка моніторингу точки доступу на AMP. Необхідно вибрати радіостанцію 802.11bgn на сторінці моніторингу AP-135-1.

Це відкриє сторінку 802.11bgn статистики радіо. Як видно на Рисунку 1.16, повідомляється про проблему з високим рівнем шуму. Причиною високого рівня

шуму є наявність широкосмугового пристрою із зафіксованою частотою. Графіки рівня шуму та використання каналів підтверджують, що це проблема.

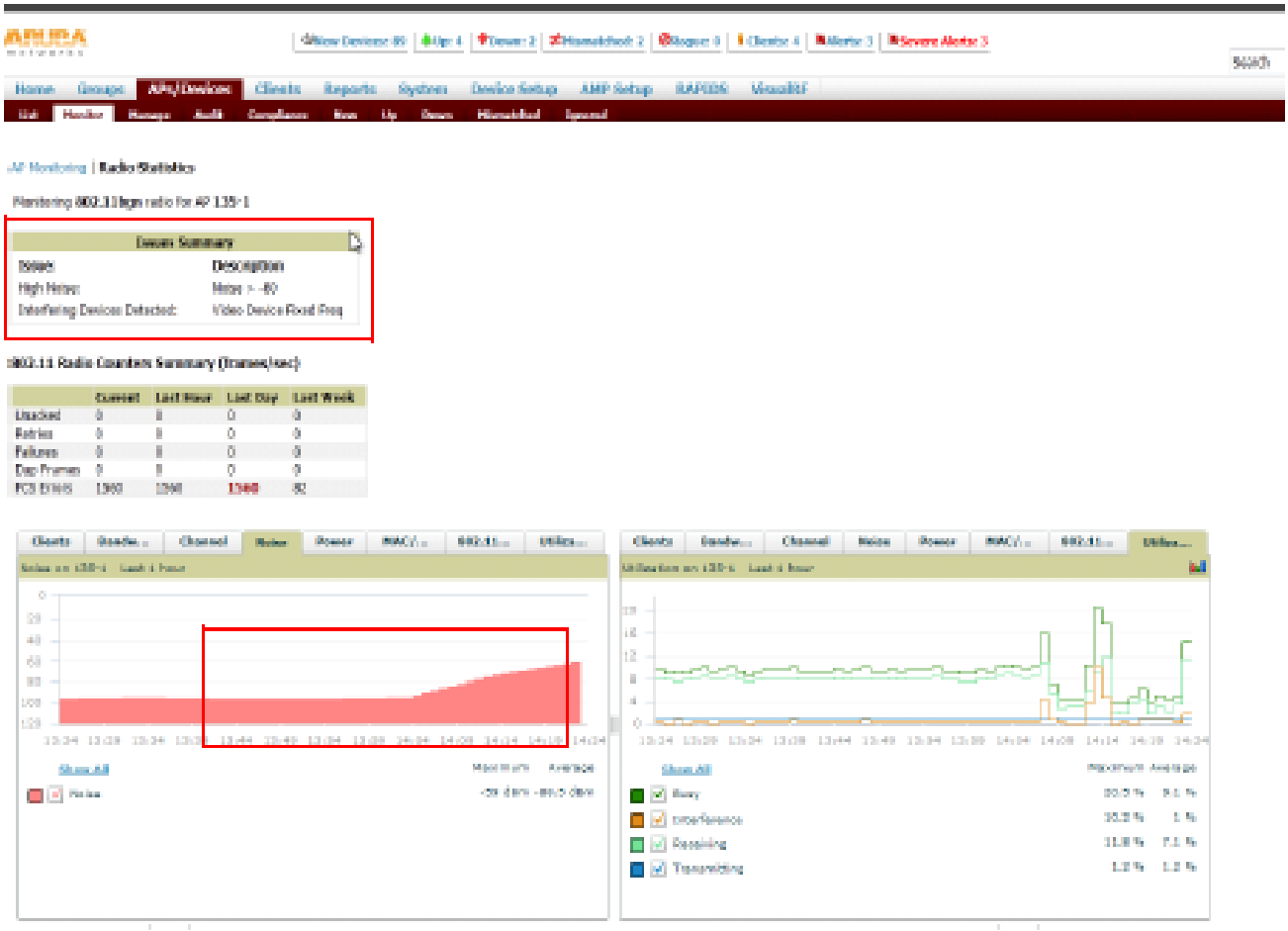

Рисунок 1.16 Використання сторінки радіо статистики для усунення несправностей у режимі реального часу

Таблиця пристроїв, що здійснюють інтерференцію, на сторінці статистики радіо надає інформацію, що стосується інтерференції, що дозволяє адміністратору визначити робочий цикл джерела шуму та задіяних каналів. Це дозволяє адміністратору визначити, чи є це постійним або тимчасовим джерелом шуму з позначками часу першого/останнього бачення

Три точки доступу в мережі здатні чути відеомсст на різних рівнях сигналу. За допомогою тріангуляції сили сигналу місце розташування перешкоди можна наблизити до плану поверху. Сторінка моніторингу точки доступу на AMP має посилання на візуальний RF-модуль. Необхідно вибрати карту.

Це відкриває план поверху модуля Visual RF із розташуванням трьох точок доступу та пов'язаних клієнтів. Відеоміст у діапазоні 2,4 ГГц був ідентифікований і розміщений на плані поверху як показано на Рисунку 1.17.

Рисунок 1.17 Відстеження місцезнаходження інтерференції на AMP

На скріншоті нижче є 4 різні діаграми для візуалізації, а саме FFT в режимі реального часу, робочий цикл FFT, спектрограма та активні пристрої. З опису кожної діаграми, згаданого в попередньому розділі, видно, що канал 11 бомбардується високою енергією та джерелом інтерференціїіз великим робочим циклом, як показано на Рисунку 1.18.

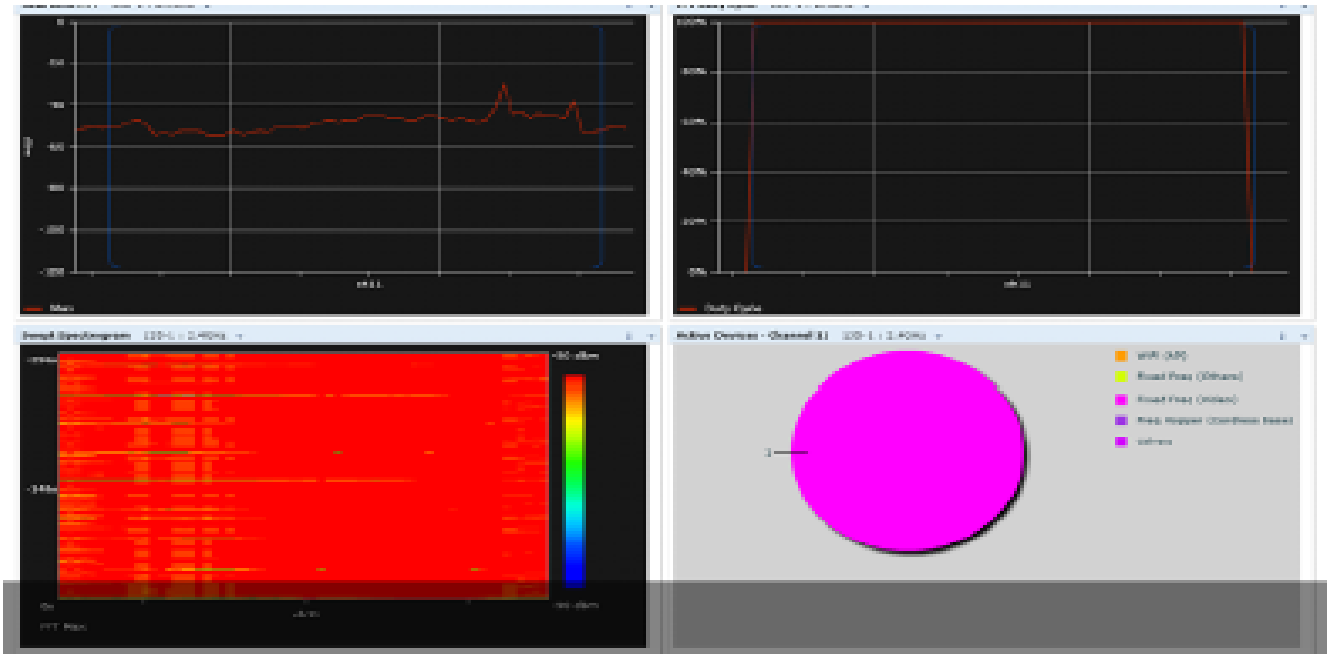

Рисунок 1.18 Аналіз спектру для ураженої АР (АР-135-1)

Aruba WLAN надає попередження в режимі реального часу, RF статистику, виявлення інтерференції, класифікацію, візуалізацію місця розташування та спектру. Тепер адміністратор WLAN має достатню кількість інформації, необхідної для того, щоб спуститися до району, де знаходився пристрій, і вимкнути його, тим самим відновивши надійні радіочастотні умови для офісу.

Таким чином, можна зробити висновок, що безпроводова локальна мережа Aruba надає вікно у радіочастотне середовище, яке забезпечує видимість джерел інтерференції та проблем, які можуть призвести до погіршення продуктивності. Без рішення інтегрованого аналізу спектра адміністраторам цих систем практично неможливо ізолювати перешкоди на сайтах із високою щільністю клієнта, мультимедійних додатках, чутливих до затримок, або електромагнітно складних RF середовищах. Це основа для широкого спектру послуг, що покращує продуктивність та функціональність безпроводової локальної мережі.

Включення AMP в архітектуру вводить такі важливі функції, як усунення несправностей у режимі реального часу, відстеження місцезнаходження джерел перешкод, звіти про стан активного пошуку несправностей та історію подій. Адміністратор WLAN тепер має доступ до радіочастотного середовища, а використання інтегрованого рішення для аналізу спектра та управління мережею здатне суттєво допомогти у вирішенні проблем.

Але лише у поєднанні з технологією Adaptive Radio Management (ARM) аналізатор спектра повністю автоматизує виявлення, класифікацію та пом'якшення інтерференції, не вимагаючи ручного втручання або додаткового обладнання.

2 ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ ARUBA ADAPTIVE RADIO MANAGEMENT (ARM) ДЛЯ ОПТИМІЗАЦІЇ РАДІОЧАСТОТНОГО РЕСУРСУ БЕЗПРОВОДОВОЇ МЕРЕЖІ

2.1. Дослідження роботи алгоритму автоматичної адаптації радіочастотного середовища Aruba Adaptive Radio Management (ARM)

Радіочастотний (РЧ) спектр - це обмежений та спільний ресурс і для забезпечення оптимального досвіду для користувачів необхідно контролювати якомога більше факторів. Функція Aruba Adaptive Radio Management (ARM) - це набір інструментів, які дозволяють інфраструктурі WLAN приймати рішення про радіоресурси та підключення клієнтів без ручного втручання адміністраторів мережі або програмного забезпечення на стороні клієнта.

Aruba використовує інформацію, зібрану з точок доступу та моніторів ефіру (AM), які сканують радіочастотне середовище, щоб надавати інформацію алгоритмам та службам ARM. Інфраструктура має загальномережний огляд точок доступу та клієнтів і ця інформація використовується для оптимізації мережі та забезпечення покращеної роботи клієнта. ARM є частиною базової ArubaOS ™ і доступна на всіх контролерах мобільності та точках доступу Aruba.

Коли було вперше впроваджено WLAN 802.11, мережевим адміністраторам довелося вручну будувати канал і план живлення на основі одноразового опитування сайту. Після налаштування точок доступу вони залишались у цьому стані, доки адміністратор не змінював налаштування.

Коли ми обговорюємо клієнтів та точки доступу, важливо вказати діапазон, на якому може працювати кожен. Для окремих радіоточок AP категорізація становить 802.11a/n/ac для 5 ГГц та 802.11b/g/n для 2,4 ГГц, що означає, що швидкості та функції 802.11n/ac доступні у кожному діапазоні. Для інженера з досвідом роботи Wi-Fi, але нового для 802.11n/ac, може бути важко зрозуміти, що поправка не є синонімом частот, на яких працює мережа.

На Рисунку 2.1 показаний типовий план каналів 2,4 ГГц, де мережевий інженер вручну повинен встановити потужність і канал кожної точки доступу. Необхідно пам'ятати, що в діапазоні 2,4 ГГц лише три канали практичні для використання в більшості регуляторних областей. Подібний план існує і в діапазоні 5 ГГц, але, як правило, доступно більше каналів. На Рисунку 2.1 показаний типовий план з каналами 2,4 ГГц і 5 ГГц.

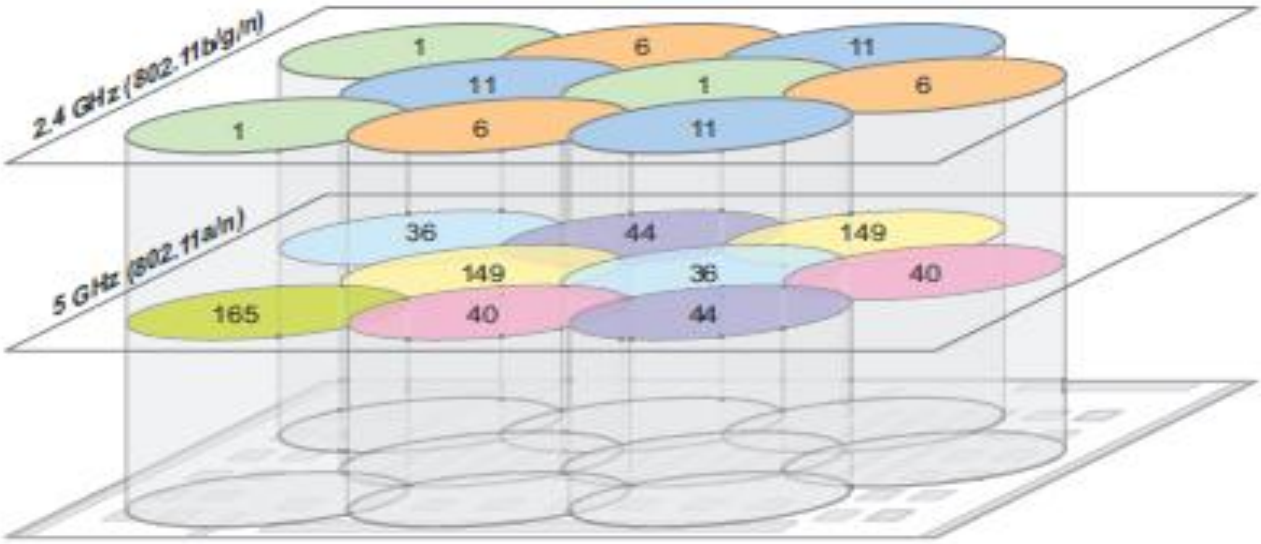

Рисунок 2.1 План каналів 2,4 ГГц і 5 ГГц

Проблема цих планів каналів полягає в тому, що вони базувались на знімку в часі радочастотного середовища. Наявність пристроїв, стін, кубів, дверей офісу, що відкриваються і закриваються, мікрохвильових печей і навіть людського тіла - все це впливає на навколишнє середовище. Це середовище рідини, як правило, не можна перевірити та компенсувати в статичному каналі та плані живлення. На Рисунку 2.2 показано теплову карту радіопокриття, як воно виглядає в реальному житті.

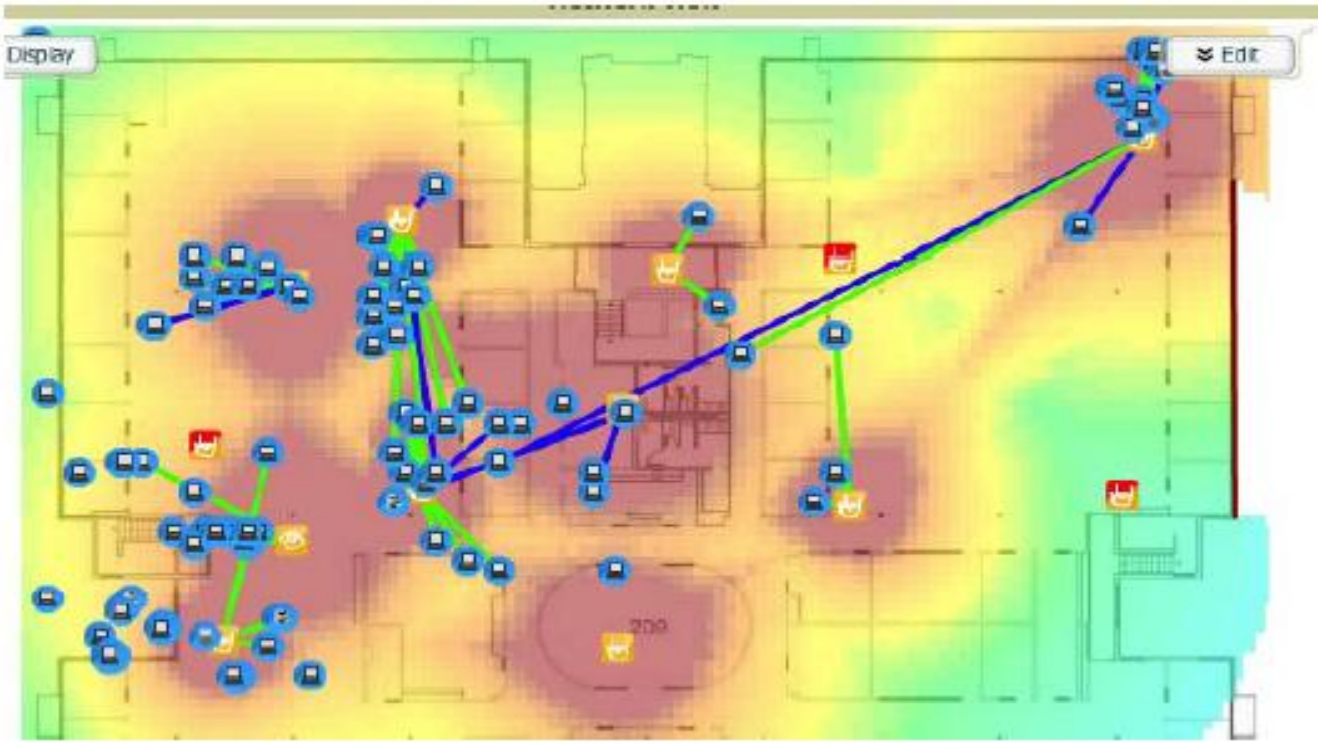

Рисунок 2.2 Типова теплова карта радіопокриття

Крім того, статичний план не працює автоматично при відмові AP і нових джерелах інтерференції. Якщо точка доступу в певній області виходить з ладу, адміністратор повинен вручну збільшити потужність навколишніх точок доступу, щоб компенсувати «дірку» радіочастотного покриття, доки цю точку доступу не можна буде замінити. Якщо постійна інтерференція робить канал непридатним для використання, ця AP повинен бути налаштований на новий канал. Нові канали, як правило, мають ефект каскаду і вимагають внесення змін в інші сусідні точки доступу в цій зоні, з часом поширюючись по всій локальній безпроводовій мережі. На Рисунку 2.3, якщо з'являється безпроводова камера, яка заважає каналу точки доступу, весь план повинен бути скоригований для компенсації.

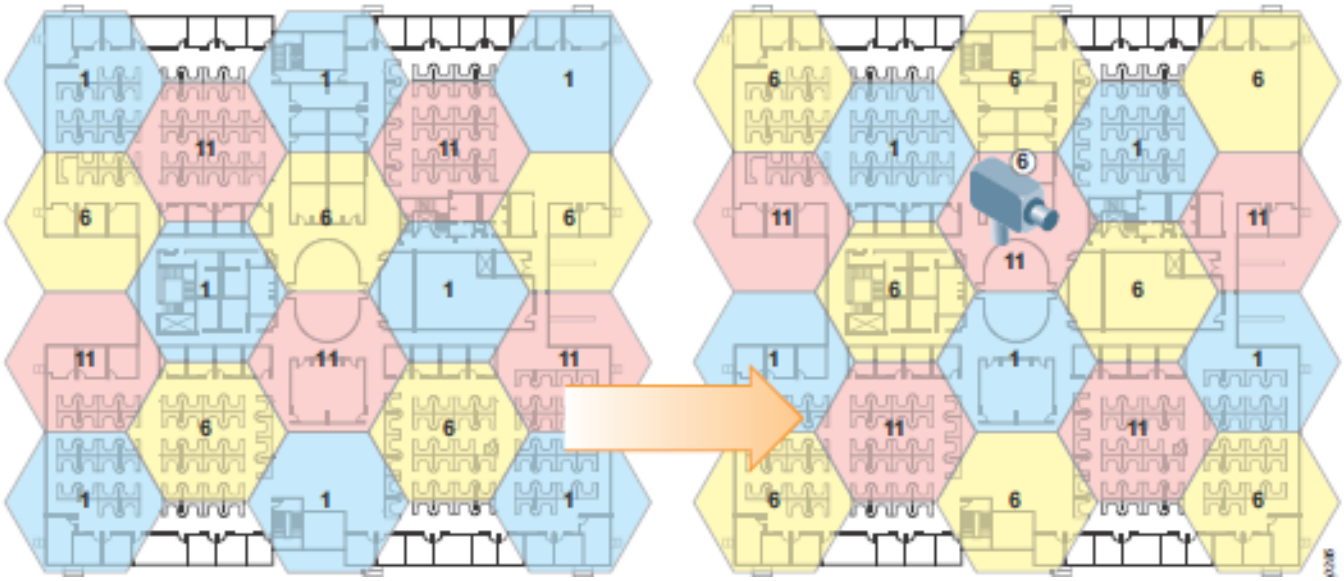

Рисунок 2.3 Без ARM зміна каналів - це трудомісткий процес, який потребує великих зусиль, щоб обійти інтерференцію

На базовому рівні ARM дозволяє мережі враховувати Wi-Fi і не Wi-Fi інтерференцію та інші AP, перш ніж налаштовувати параметри каналів для точок доступу. AP та AM постійно сканують навколишнє середовище. Якщо точка доступу виходить із ладу, ARM автоматично заповнює діру радіочастотного покриття. ARM збільшує потужність навколишніх точок доступу, поки не відновиться початкова точка доступу. Після відновлення точки доступу ARM встановлює мережу на нове оптимальне налаштування. Якщо в мережі з'являється заважаючий пристрій (Wi-Fi або не Wi-Fi), наприклад безпроводова камера, яка споживає канал, ARM належним чином налаштовує канали AP.

За деяких обставин, коли є надзвичайні перешкоди, точки доступу, які розташовані спільно, можуть бути встановлені на один і той же канал. Це часто

трапляється, коли щось на зразок IP-відеокамери використовує 100% каналу. У цьому випадку ARM може встановити точки доступу для того самого каналу, щоб обійти перешкоди. Приймається рішення надати певну послугу, навіть якщо вона зменшена, клієнтам, замість того, щоб перейти на насичений канал, який жоден клієнт не може використовувати.

Для визначення перешкод алгоритм ARM використовує декілька частин інформації, яку збирають точки доступу та модулі управління. Ці пристрої сканують усі доступні канали в домені. AP та AM збирають інформацію про інші точки доступу, клієнтів, неправдиві точки доступу, фоновий шум та перешкоди, що не стосуються 802.11. Ці розрахунки включають два індекси, які використовує ARM: індекс інтерференції та індекс покриття (Рисунок 2.4).

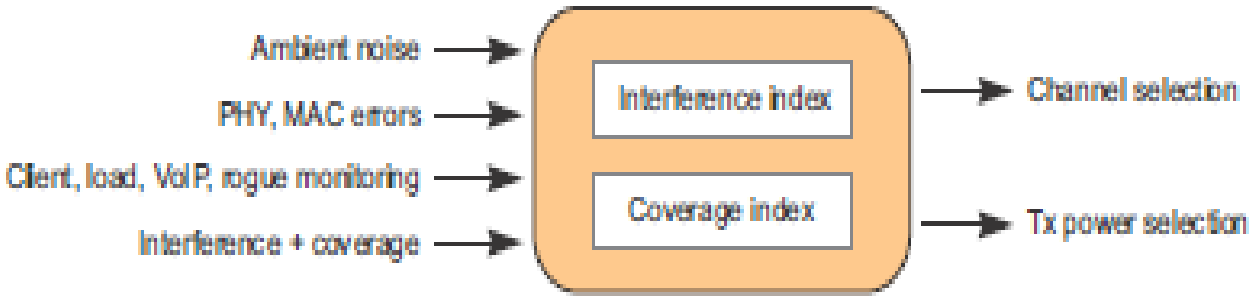

Рисунок 2.4 Індекс інтерференції та індекс покриття

Індекс інтерференції використовується для моніторингу активності каналу та інтерференції. Коли індекс інтерференції високий порівняно з іншими каналами, точка доступу хоче переключитися на канал з нижчим індексом інтерференції. Індекс покриття використовується для визначення рівнів потужності точки доступу. Точки доступу контролюють інші точки доступу на тому самому каналі і ARM встановлює рівень потужності точки доступу на основі отриманої сили передачі інших точок доступу.

ARM постійно контролює ці два показники і може автоматично адаптуватися до мінливого радіочастотного середовища. Вибір каналу та потужності регулюється автоматично, без втручання адміністратора мережі. За винятком випадків екстремальних перешкод або виявлення радіолокатора в певних каналах, точки доступу можуть бути встановлені так, щоб вони залишались на каналі, що обслуговує клієнтів, тим самим уникаючи порушення зміни каналу.

Aruba надає ряд команд для вивчення стану середовища радіопокриття. Наведені тут налаштування описують поточне середовище, яке бело досліджено на обладнанні Aruba:

```
(LC1-Sunnyvale-6000) #show ap arm rf-summary ap-name AP-LC1

Channel Summary
---------------
channel  retry  low-speed  non-unicast  frag  bwidth  phy-err  mac-err  noise  cov-idx  intf_idx
-------  -----  ---------  -----------  ----  ------  -------  -------  -----  -------  --------
161      0      0          0            0     0       0        0        93     0/0      66/71//0/0
1        0      0          0            0     0       0        11       89     15/0     351/69//0/0
48       0      0          0            0     0       0        17       89     0/0      232/89//0/0
165      0      0          0            0     0       0        0        94     0/0      0/19//0/0
5        0      0          0            0     0       0        0        87     0/0      0/469//0/0
6        0      0          0            0     0       0        8        85     0/0      415/153//0/0
7        0      0          0            0     0       0        0        79     0/0      0/520//0/0
11       0      0          0            0     0       0        11       84     0/0      519/66//0/0
149      0      0          0            0     0       0        19       85     11/0     55/42//0/0
36       0      0          0            0     0       0        6        91     0/0      277/42//0/0
153      0      0          0            0     0       0        0        81     0/0      123/85//0/0
40       0      0          0            0     0       0        0        90     0/0      125/179//0/0
```

```
157      0      0          0          0     0      0       17       90     0/0      215/64//0/0
44       0      0          0          0     0      0       55       91     0/0      267/115//0/0
HT Channel Summary
------------------
channel_pair  Pairwise_intf_index
------------  -------------------
1-5           889
7-11          1105
149-153       305
36-40         623
157-161       416
44-48         703

Interface Name           :wifi0
Current ARM Assignment   :149+/9
Covered channels a/g     :1/0
Free channels a/g        :8/0
ARM Edge State           :disable
Last check channel/pwr   :4h:46m:7s/2m:17s
Last change channel/pwr  :21h:21m:32s/8h:8m:15s
Next Check channel/pwr   :0s/2m:41s

Interface Name           :wifi1
Current ARM Assignment   :1/9
Covered channels a/g     :0/1
Free channels a/g        :0/2
ARM Edge State           :disable
Last check channel/pwr   :2m:54s/2m:44s
Last change channel/pwr  :8m:1s/19m:41s
Next Check channel/pwr   :2m:3s/2m:37s
```

У таблиці описуються зведені дані каналу, які є найбільш релевантними для розрахунку індексу інтерференції.

Column Heading	Description
Retry	The amount of 802.11 retries seen on a channel expressed (%).
Low-speed	The amount of 802.11 frames seen at a data rate of 18 Mb/s or lower expressed (%).
Non-unicast	The amount of broadcast/multicast frames seen on the channel (%).
Frag	The amount of fragmented frames seen on a channel (Kb/s).
Bwidth	The amount of throughput seen on a channel (Kb/s).
Phy-err	The amount of frames with physical errors seen on a channel (%).
Mac-err	The amount of frames with MAC errors seen on a channel (%).
Noise	The APs noise floor (0 dBm).
Cov-idx	The amount of RF coverage from valid Aruba APs on a specific channel (#).
Intf_idx	An 802.11 RF interference summary that is categorized into four values: • Single channel interference is calculated by the AP • Interference from APs on adjacent overlapping channels is calculated by the AP • Single channel interference reported by neighboring APs • Interference on adjacent overlapping channels is reported by neighboring APs

Усі точки доступу Aruba можуть виконувати сканування, але точки доступу, які обслуговують клієнтів та оперативні органи виконують свої обов'язки щодо сканування по-різному. Програмний модуль Aruba RFProtect також змінює режими сканування завдяки введенню функції TotalWatchTM.

Сканування за допомогою AP.

Основною функцією AP є обслуговування клієнтів. Однак вона також сканує ефір з наступних причин:

шукає кращі канали;

моніторить події системи виявлення вторгнень (IDS);

прослуховує клієнтів;

здійснює пошук зловмисних пристроїв;

бере участь у стримуванні зловмисних дій.

За замовчуванням точка доступу сканує свій поточний канал у звичайному режимі роботи та вимикає канал для сканування кожні 10 секунд. AP витрачає 85 мілісекунд сканування поза каналом, скануючи його приблизно 65 мілісекунд із 20 мілісекундами накладних витрат, що використовуються в якості радіозміни каналів, а потім повертається до свого домашнього каналу.

Стримування зловмисних пристроїв виконується лише на домашньому каналі точки доступу, якщо не ввімкнено сканування з урахуванням зловмисних пристроїв.

Сканування за допомогою AM.

Сканування AM схоже на сканування AP, за винятком того, що AM постійно сканує інші мережі і не обслуговує клієнтів. AM слухає та передає лише те, що містить зловмисні точки доступу або клієнтів. Коли AM розгортаються на апаратному забезпеченні точки доступу, яке має лише одне радіо, AM чергується між діапазонами 2,4 і 5 ГГц на одному радіо AP. Коли зловмисник повинен бути утриманий, AM може витратити більше часу на утримання зловмисника, ніж сканування, що призводить до більш послідовного затримання.

AM використовує той самий зважений алгоритм для сканування каналів, і він віддає перевагу каналам, які мають активних користувачів та трафік. AM проводить додатковий час на тих каналах, на відміну від каналів, які не мають активності.

Сканування AM модифіковано ліцензією RFProtect. Aruba рекомендує застосовувати приблизно одну AM на кожні чотири розгорнуті точки доступу AP, щоб забезпечити ефективне стримування. Для підвищення точності при

використанні служб визначення місцезнаходження та збільшення можливості виявлення загроз ззовні фізичної будівлі, Aruba також рекомендує розміщувати AM по внутрішньому периметру будівлі. У той час як AP доповнюють AM для ідентифікації неправдивих, для стримування є кращими виділені AM.

Для підвищення точності при використанні служб визначення місцезнаходження та збільшення можливості виявлення загроз ззовні фізичної будівлі, Aruba також рекомендує розміщувати AM по внутрішньому периметру будівлі. У той час як AP доповнюють AM для неправдивих ідентифікацій, для стримування кращими є виділені AM.

Час сканування каналів (базова ОС).

Для розрахунку часу сканування спочатку потрібно встановити час циклу. Спочатку всі регуляторні доменні канали скануються з однаковою вагою. Точка доступу з радіостанцією 2,4 ГГц на каналі 1 сканує канали таким чином: 1-2-1-3-1-4-1-5-1-6 тощо, поки не будуть скановані всі канали. AM просто сканує всі канали, 1-2-3-4-5-6, поки не просканує всі доменні канали.

Після першого проходження через регуляторні доменні канали цей шаблон змінюється на зважений алгоритм. Активним каналам надається більше ваги в системі і вони скануються частіше, ніж канали, де точка доступу не спостерігає користувачів та трафік. За замовчуванням скануються всі легальні канали у всіх регуляторних доменах. У наведеному нижче списку показано порядок алгоритму сканування AP та AM без ліцензії RFProtect:

1. Active channel
2. Active channel
3. Active channel
4. Regulatory domain channel
5. Active channel
6. Active channel
7. Active channel
8. Regulatory domain channel
9. Other regulatory domain channel
10.Active channel
11.Active channel
12.Active channel
13.Regulatory domain channel
14.Active channel
15.Active channel
16.Active channel

17.Regulatory domain channel

18.Other regulatory domain channel

19.Repeat pattern

Щоб розрахувати час, який потрібно для сканування усіх каналів після початкового проходу сканування, спочатку необхідно обчислити час, який необхідно для переходу через всі 18 кроків, показаних вище, плюс час, витрачений на обслуговування клієнтів:

*(((12 active channels * scan time) + (4 regulatory channels * scan time) + (2 other regulatory domain channels * scan time)) * .001) + 180 seconds for APs only (time spent on channel)*

Таким чином, AP займає стільки часу:

*(((12 * 85) + (4 * 85) + (2 * 85)) * .001) + 180 = 181.53 seconds*

А AM вимагає стільки часу:

*(((12 * 500) + (4 * 250) + (2 * 200)) * .001) = 7.4 seconds*

Тепер, коли час циклу відомий, можна розрахувати кількість часу, необхідного для циклу по всіх інших регуляторних доменних каналах. AP або AM сканує чотири регуляторних доменних каналів за цикл. Точки доступу 802.11n також сканують канали +/- 40 МГц, що вимагає двох сканувань на канал.

*(Number of channels in the regulatory domain/4 regulatory domain channel scans per pass) * 2 for 40 MHz +/- * cycle time*

Точка доступу, яка потребує сканування 11 каналів 2,4 ГГц з використанням часу попереднього циклу, вимагає стільки часу:

*11/4) * 2 * 181.53 = 998.4 seconds, or about 16 minutes*

Для сканування AM для тих самих 11 каналів потрібно стільки часу:

*(11/4) * 2 * 7.4 = 40.7 seconds, or .7 minutes*

Враховуючи ці розрахунки, можна визначити час сканування для AP та AM. У таблиці перелічено час сканування для базової ОС. Ця таблиця передбачає 14 каналів в діапазоні 2,4 ГГц і 28 каналів в 5,0 ГГц.

AP 2.4 GHz	AP 5 GHz	Single-Radio AM	Dual-Radio AM
16.6 min	42.4 min	2.4 min	1.7 min

Односмугове та багатосмугове сканування (Single-Band and Multiband Scanning).

Параметр ARM для сканування визначає, як відбувається сканування. Для точок доступу з двома радіостанціями слід вибрати односмугове сканування (за замовчуванням). Для точок доступу з одним радіо за замовчуванням має бути багатосмугове сканування, яке дозволяє точці доступу сканувати діапазони частот 2,4 ГГц та 5 ГГц.

Модифікація сканування ARM та зміни каналів.

Сканування ARM зазвичай не призводить до того, що клієнт пропускає передачу. Однак у деяких випадках може бути вигідно призупинити сканування на певний час. Крім того, у певних випадках зміна каналів може бути більш руйнівною, ніж залишатися на неоптимальному каналі. Призупинення сканування ARM та змін каналів є необов'язковим і може бути ввімкнено залежно від потреб розгортання.

Існують певні випадки, коли призупинення сканування ARM буде замінено. Коли точка доступу стикається з екстремальними стійкими перешкодами, які роблять канал непридатним для клієнтів, точка доступу перемикає канали навіть з увімкненим призупиненням ARM. Точки доступу, які використовують DFS, завжди змінюють канали, коли виявляють наявність радіолокатора на каналі.

Клієнтський режим ARM (Client-Aware ARM).

Клієнтський режим ARM не дозволяє точці доступу змінювати канали, коли активний клієнт пов'язаний. Цей режим увімкнено за замовчуванням. Якщо ARM, відома клієнтові, вимкнена, AP може змінювати канали, навіть коли клієнти пов'язані, що змушує цих клієнтів повертатися назад через процес асоціації. Aruba рекомендує активувати ARM з урахуванням клієнтів для всіх розгортань.

Голосове сканування (Voice-Aware Scanning).

На відміну від більшості передач даних, голосові дзвінки дуже чутливі до втрат, тремтіння, випадіння пакетів та відсутності відповіді з точки доступу. Коли використовується Voice over Wi-Fi, слід увімкнути режим голосового сканування, щоб запобігти скануванню точки доступу під час активного голосового дзвінка. Контролер мобільності стежить за трафіком, позначеним як голос з міткою QoS/Wi-Fi Multimedia ™ (WMM®). Крім того, брандмауер стану Aruba використовується для розрізнення активного голосового сеансу від пов'язаного голосового клієнта. На час активного дзвінка система призупиняє сканування точки доступу, яка обслуговує клієнта.

Щоб запобігти скануванню точки доступу поза каналом, поки активні інші програми з високим пріоритетом (наприклад, монітори пацієнтів в охороні здоров'я), використовуйте брандмауер Aruba, щоб аналогічно позначити трафік для пріоритету голосового QoS/WMM та затримати сканування. Aruba рекомендує ввімкнути голосову ARM для всіх розгортань.

Відео сканування (Video-Aware Scanning).

Подібно до голосового сканування, відео сканування шукає трафік, який позначений як відеотрафік WMM/QoS. Під час передачі відео сканування призупиняється, щоб клієнт отримав високоякісний відеопотік. Aruba рекомендує ввімкнути ARM з підтримкою відео для всіх розгортань.

Сканування з урахуванням навантаження (Load-Aware Scanning).

За нормальної роботи, точки доступу сканують поза каналом як частину своїх обов'язків у мережі WLAN. Іноді трафік пропускається, але клієнт просто повторно надсилає ці дані, коли не отримує підтвердження. Зі збільшенням навантаження клієнта та трафіку на AP, ці ретрансляції використовують все дефіцитніший ефірний час. Коли навантаження трафіку переходить настроюваний поріг, ARM призупиняє сканування на цій точці доступу. Коли навантаження трафіку опускається нижче порогового значення, точка доступу поновлює сканування. Aruba рекомендує ввімкнути сканування з урахуванням навантаження для всіх розгортань із типовим значенням 10 Мбіт/с.

Енергозберігаюче сканування (Power-Save-Aware Scanning).

У цьому режимі точка доступу не сканує, коли один або кілька клієнтів перебувають у режимі енергозбереження. Цей режим був розроблений насамперед для обробки одномодових голосових слухавок. Оскільки клієнти еволюціонували, майже всі клієнти тепер вводять режим енергозбереження, коли вони не підключені до джерела живлення. Коли клієнти переходять у режим енергозбереження, точка доступу не може змінювати канали. Зараз Aruba рекомендує вимкнути цю функцію на користь голосового сканування.

Сканування з урахуванням зловмисників (Rogue-Aware Scanning).

Сканування з урахуванням зловмисників було розроблено для середовищ із високим рівнем безпеки, де стримування шахраїв є критичним. Коли ввімкнено сканування з урахуванням зловмисників, точка доступу змінить канали, щоб містити зловмисників, якщо жоден клієнт не підключений активно та не ввімкнута ARM з урахуванням клієнтів. Aruba рекомендує увімкнути сканування з урахуванням зловмисників лише для середовищ із високим рівнем безпеки і повинно вмикатись лише спільно з ARM з урахуванням клієнтів, про які вже йшлося раніше.

2.2. Дослідження механізму динамічного розподілу безпроводових клієнтів по діапазонах

Керування механізму динамічного розподілу безпроводових клієнтів по діапазонах ARM (band steering) вирішує конкретну проблему, пов’язану з драйверами на пристроях, здатних функціонувати в обох діапазонах. На більшості дводіапазонних клієнтських пристроїв драйвер шукає з'єднання в діапазоні 2,4 ГГц, перш ніж шукати один із 5 ГГц. Незважаючи на те, що пристрій може працювати в обох діапазонах, 2,4 ГГц є найбільш часто доступним діапазоном, тому пристрій спочатку шукає з'єднання в цьому діапазоні. Клієнти можуть також бачити посилений сигнал з частоти 2,4 ГГц, коли вони перебувають на межі діапазону покриття для безпроводової локальної мережі.

Функція динамічного розподілу безпроводових клієнтів по діапазонах ARM (band steering) визначає пристрої, які підтримують подвійний діапазон і вона реагує на ці пристрої лише в діапазоні 5 ГГц. Функція динамічного розподілу безпроводових клієнтів по діапазонах ARM (band steering) може спонукати або змусити пристрої переміщатися на смугу частот 5 ГГц, яка має більше доступних каналів, більшу пропускну здатність і спричиняє менше інтерференції для користувачів (Рисунок 2.5).

Динамічний розподіл безпроводових клієнтів по діапазонах вимагає рівного покриття між діапазонами 2,4 ГГц і 5 ГГц, щоб бути ефективним. Більша модель покриття 2,4 ГГц призводить до непередбачуваних результатів для клієнтів, особливо якщо використовується робочий режим із посиленням 5 ГГц. Вивчіть покриття мережі, використовуючи VisualRF ™ Plan, перш ніж увімкнути динамічний розподіл безпроводових клієнтів по діапазонах в режимі сили 5 ГГц. Нові мережі слід планувати, використовуючи модель покриття 5 ГГц і розгортати їх з дворежимними точками доступу в кожному місці. Це розгортання дозволяє ARM зменшити потужність на 2,4 ГГц, щоб компенсувати щільне розгортання. Надмірне проектування діапазону 2,4 ГГц необхідне для ефективного використання діапазону рульового управління.

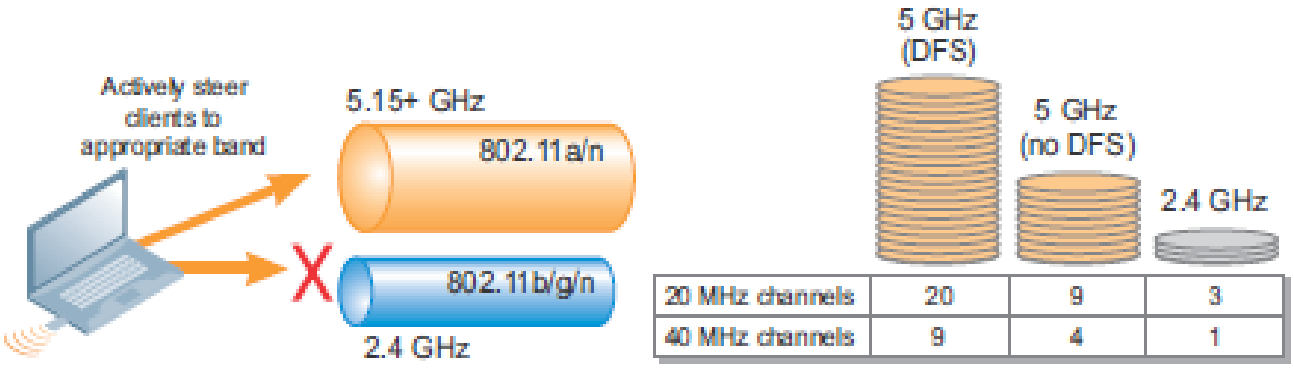

Рисунок 2.5 Дводіапазонні пристрої спрямовані на діапазон 5 ГГц

У таблиці нижче описані різні режими, які доступні, коли ввімкнено динамічний розподіл безпроводових клієнтів по діапазонах.

Mode	**Description**
Balance Bands	Спроби збалансувати клієнтів у приблизному співвідношенні чотирьох клієнтів 5 ГГц для кожного клієнта 2,4 ГГц.
Prefer 5 GHz (default)	Цей режим є стандартною операцією для системи. Клієнтам, які можуть працювати на частоті 5 ГГц, рекомендується перейти на діапазон 5 ГГц. Якщо клієнт продовжує намагатися працювати на частоті 2,4 ГГц, навіть коли йому пропонується з'єднання 5 ГГц, система дозволяє їм підключатися на частоті 2,4 ГГц. Aruba рекомендує ввімкнути режим віддавати перевагу 5 ГГц (Prefer 5 GHz) для всіх розгортань.
Force 5 GHz	Подібно до режиму роботи віддавати перевагу 5 ГГц (Prefer 5 GHz), але Force 5 ГГц вимагає, щоб точка доступу відповідала клієнту лише на частоті 5 ГГц, без винятків.

Балансування спектрального навантаження (Spectrum Load Balancing).

У щільних розгортаннях AP, навіть якщо ввімкнено динамічний розподіл безпроводових клієнтів по діапазонах, клієнтам у кожному діапазоні збалансувати всі доступні канали є ідеалом. Балансування спектрального навантаження переміщує клієнтів з сильно перевантажених точок доступу та каналів на точки доступу та канали в тій же околиці, які навантажені легше. Цей процес відрізняється від простого балансування навантаження, оскільки береться до уваги і канал AP, до якого спрямовується клієнт. Використовуючи весь доступний спектр, суперечка клієнтів щодо пропускної здатності може бути значно зменшена. Aruba рекомендує ввімкнути балансування навантаження спектра лише при щільному розгортанні точок доступу. Aruba не рекомендує вмикати цю функцію для голосового розгортання, натомість покладаючись на функції контролю прийому дзвінків.

Режим ARM (Mode-Aware ARM).

У багатьох випадках подвійні режими точки доступу (ті, що мають як 2,4, так і 5 ГГц радіо) розгортаються в дуже щільних середовищах для підтримки великої кількості користувачів. Хоча це розгортання працює дуже добре в більшості випадків завдяки налаштуванню ARM, в деяких ситуаціях радіопередачі можуть заважати один одному через відстань, яку проходить

сигнал. Ця перешкода представлена як міжканальна інтерференція (co-channel interference - CCI) та інтерференція сусіднього каналу (adjacent channel interference - ACI). Ця інтерференція найчастіше зустрічається на частоті 2,4 ГГц, хоча вона може виникати і в дуже щільних розгортаннях на частоті 5 ГГц. Коли ввімкнено динамічний розподіл безпроводових клієнтів по діапазонах, менша кількість клієнтів використовуватиме діапазон 2,4 ГГц, тому потрібно менше радіостанцій 2,4 ГГц Рисунок 2.6).

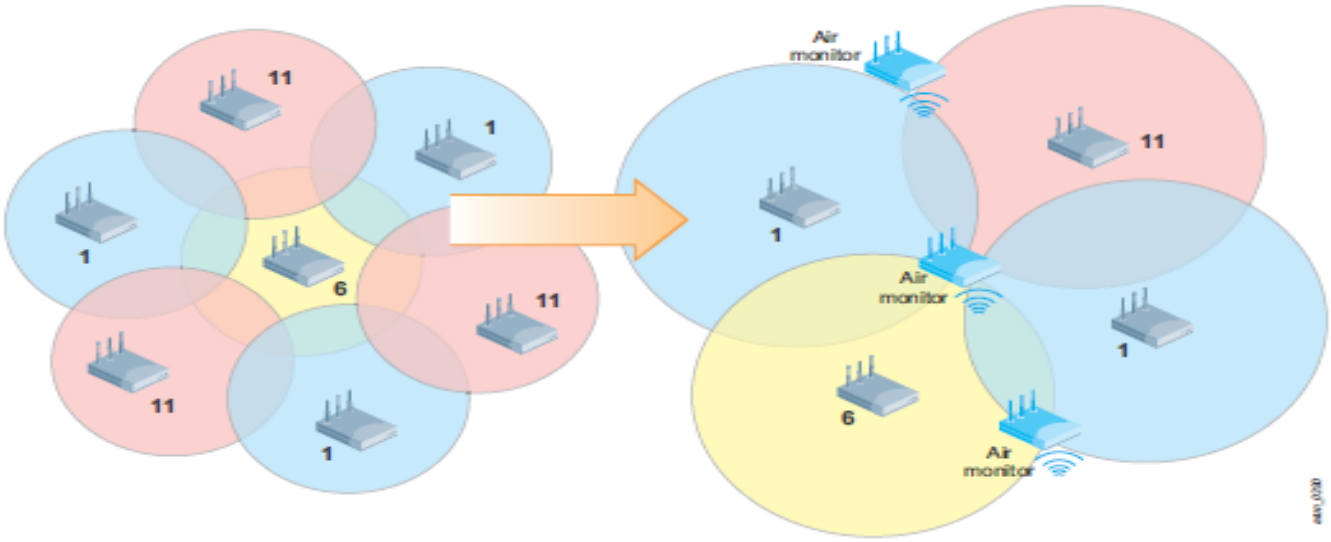

Рисунок 2.6 Щільне розгортання до та після включення ARM із підтримкою режиму

У цих випадках, коли точки доступу не потрібні для обслуговування клієнтів, а CCI або ACI збільшуються, може бути вигідно змінити деякі радіостанції на AM. Як правило, радіостанції 2,4 ГГц змінюються на AM через велике поширення сигналу та обмежену кількість каналів. Режим ARM перевіряє поточне навантаження мережі та інтерференція від передач AP, а потім переміщує точки доступу в режим AM. ARM, що відповідає режиму, знає про “крайові” точки доступу і не перетворює їх на AM. Крайові точки доступу не слід переключати на AM, оскільки, якщо вони припиняють обслуговувати клієнтів, з’являються “діри” покриття. У більшості випадків Aruba рекомендує режим ARM лише для вирішення проблем із підключенням клієнта, таких як розгортання голосу, коли наявність занадто великої кількості SSID може перевантажити клієнтські пристрої.

2.3. Дослідження механізму регулювання чутливості прийому точок доступу у щільному розгортанні

Чутливість прийому (Adjusting Receive Sensitivity) безпроводового пристрою є мірою того, наскільки пристрій може приймати та декодувати передачу. Висока чутливість прийому має сенс у ситуаціях, коли доступно мало точок доступу, наприклад, безпроводовий маршрутизатор у невеликому офісі. У цих випадках точка доступу охоплює велику територію і повинна мати можливість приймати слабкий сигнал. На Рисунку 2.7 показано типовий невеликий офіс з однією точкою доступу, який намагається забезпечити покриття всієї площі.

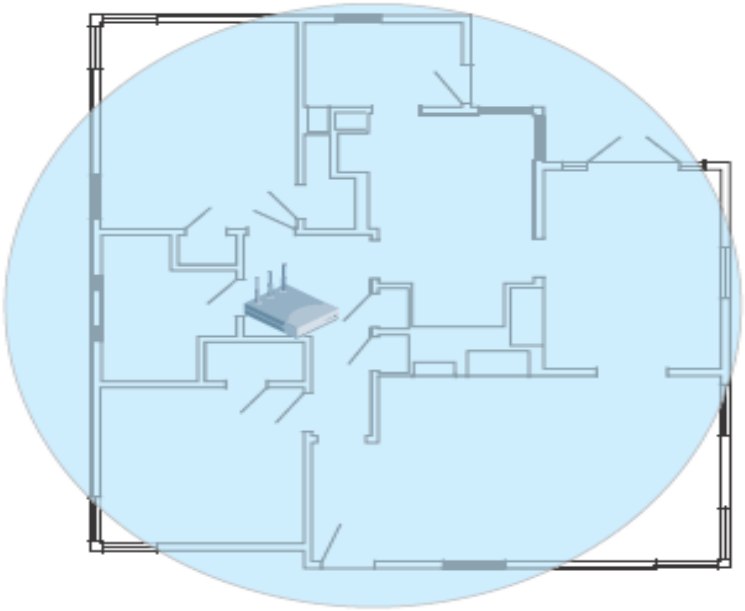

Рисунок 2.7 Одна AP з високою чутливістю прийому

Але в мережі WLAN високої щільності, у першу чергу в глядацькій залі чи на стадіоні, висока чутливість до прийому може бути непродуктивною. Щоразу, коли AP може приймати і декодувати сигнал, він повинен припинити передачу по каналу, інакше відбудеться колізія. Крім того, оскільки чутливість прийому точки доступу, як правило, перевищує чутливість клієнтів у цій зоні, колізії можуть відбуватися через приховані вузли. На Рисунку 2.8 показано, як кілька клієнтів і вузлів можуть перешкоджати один одному.

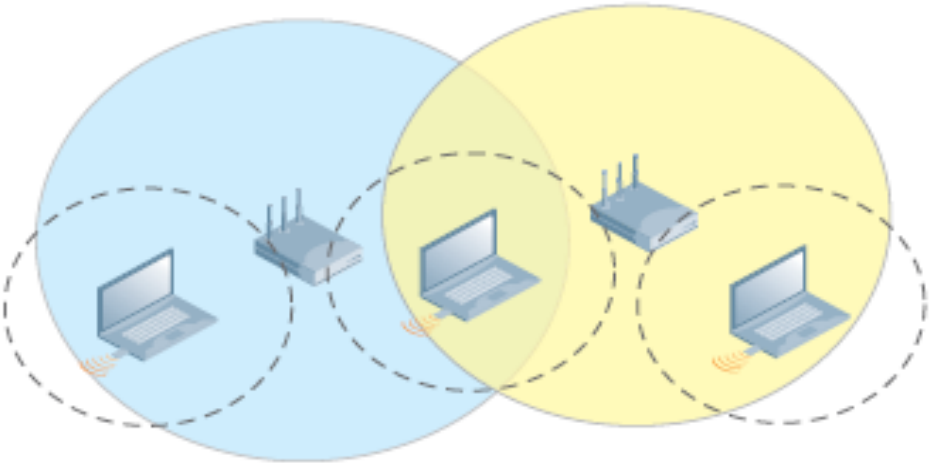

Рисунок 2.8 Приховані вузли виникають там, де точки доступу чують декількох клієнтів, які не чують один одного

У типовому щільному розгортанні точки доступу не вимагають обслуговування клієнтів на великій відстані, а висока чутливість прийому призводить до більших колізій під час передачі клієнта. ARM пом'якшує цю проблему, регулюючи чутливість прийому точки доступу на основі клієнтів, які підключені до точки доступу. ARM вимірює отримані сигнали від клієнтів, а потім регулює чутливість прийому відповідно до найгіршого підключення клієнта. Для розрахунку використовується ковзне середнє, щоб визначити правильне значення. На Рисунку 2.9 показано, як зменшений розмір комірки може допомогти запобігти прихованим проблемам вузлів.

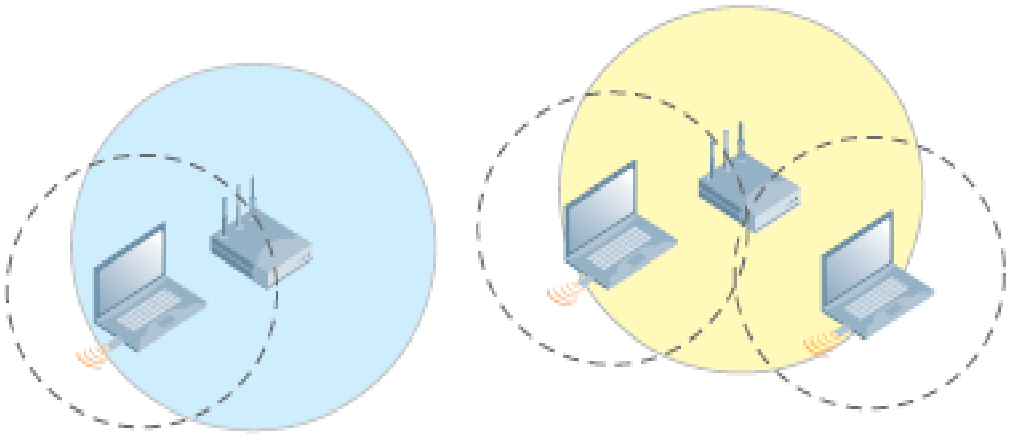

Рисунок 2.9 Динамічно налаштована чутливість прийому зменшує область колізій

ARM зменшує чутливість прийому точки доступу, так що передачі, які раніше були декодовані як законні, тепер відображаються для точки доступу як фоновий шум. Клієнти відчувають кращу пропускну здатність завдяки міжканальної інтерференції, що допомагає усунути те, що могло б розглядатися як колізії передач по повітрю.

Для зменшення чутливості точки доступу, ефективність клієнта також повинна бути зменшена. У більшості випадків увімкнення цієї функції не дасть користувачеві очікуваного результату без планування та підтримки клієнта.

Станція, яка намагається приєднатися до будь-якої WLAN, може шукати доступні безпроводові мережі, виконуючи активне сканування або пасивне сканування. Під час пасивного сканування клієнт прослуховує кадри маяків, відправлені точками доступу на кожному можливому каналі, щоб виявити доступні безпроводові мережі. Під час пасивного сканування станція повинна почекати, поки вона почує маяк з точки доступу.

Під час активного сканування клієнт надсилає запит зонду для виявлення присутності точки доступу в каналі. Кожна AP, який почує запит зонду, повинна відповісти відповіддю зонда. Відповідь зонду надає клієнтові всю необхідну інформацію про мережу, що транслюється AP. У щільному середовищі деякі клієнти можуть вирішити приєднатися до точки доступу із нижчим SNR, навіть за наявності AP з кращим SNR. Місцева функція порогового значення зонда визначає значення SNR, нижче якого точка доступу ігнорує вхідні запити зондування. Як результат, клієнти отримують відповідь зонду лише від точок доступу, які мають хороший SNR для клієнта. Ця функція заохочує правильний роумінг у щільних розгортаннях. Підтримуваний діапазон для значення SNR становить 0-100 дБ. Значення 0 вимикає цю функцію. Aruba рекомендує вмикати цю функцію в щільних середовищах зі значенням, встановленим на 25 дБ.

Інтелектуальна адаптація швидкості передачі (Intelligent Rate Adaptation).

Коли клієнту не вдається успішно передати кадр, стандарти говорять, що станція повинна перейти на нижчу швидкість передачі, поки кадр не буде успішно відправлений або до досягнення межі повторної спроби. Несправність може бути також спричинена колізіями або короткочасною інтерференцією. У цих випадках мало сенсу переходити на нижчу швидкість передачі для тимчасової події. Зміщення має побічним ефектом зменшення доступного ефірного часу для всіх користувачів, оскільки передача з меншою швидкістю передачі даних вимагає більше часу для передачі одного і того ж кадру. На Рисунку 2.10 показана економія часу, досягнута динамічним повтором спроби з більшою швидкістю, на відміну від автоматичного пониження швидкості передачі.

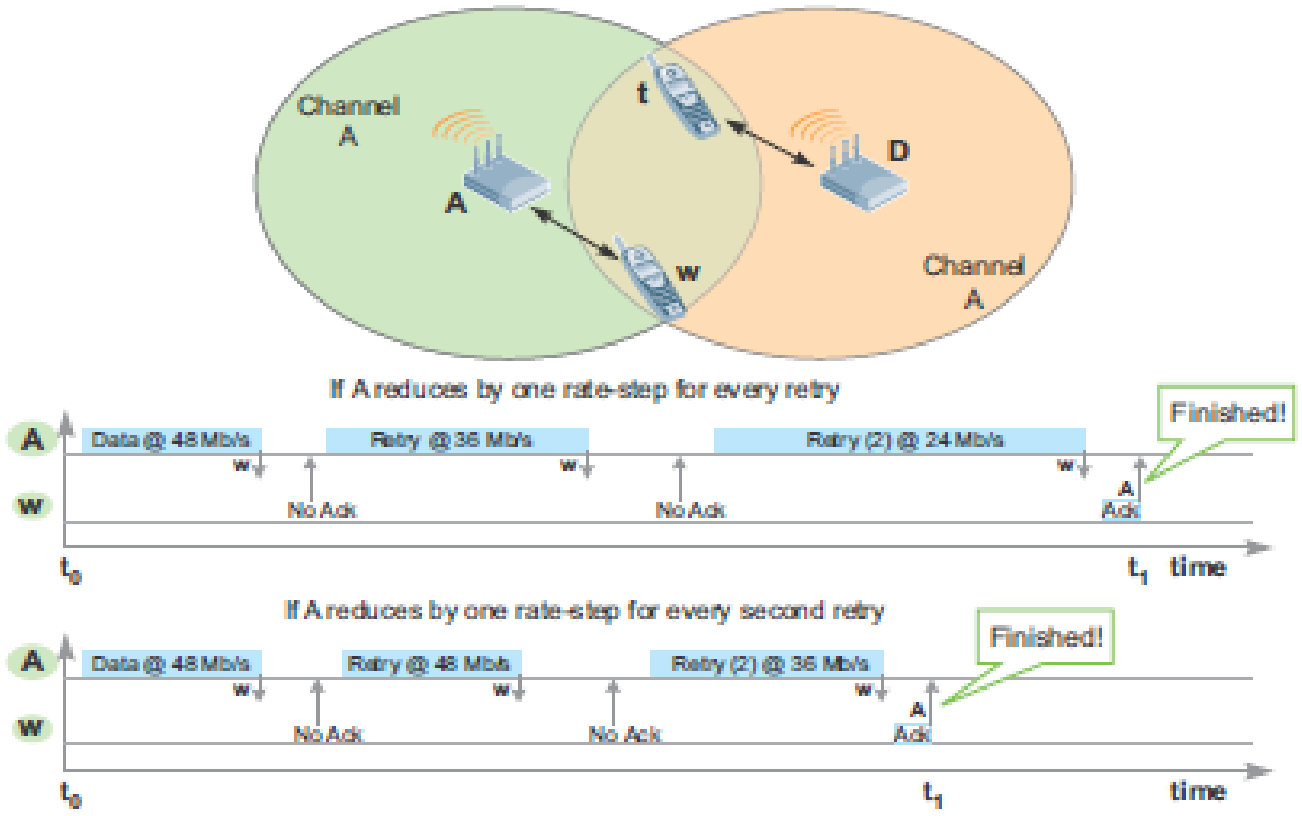

Рисунок 2.10 Передачі з меншими швидкостями передачі даних споживають більше ефірного часу

Замість того, щоб постійно знижувати швидкість при кожній повторній спробі кадру, ARM замість цього підтримує вищу швидкість передачі, що, в свою чергу, зменшує загальний час повторної спроби та спожитий час. Алгоритм працює, досліджуючи причину несправності, а не просто реагуючи на неї. Коли визначається, що збій стався через перехідний фізичний стан, такий як колізії або короткочасне джерело інтерференції, станція підтримує високу швидкість передачі даних. Інтелектуальна адаптація швидкості завжди ввімкнена, і це не можна налаштувати.

2.4. Дослідження механізму динамічної оптимізації багатоадресного трафіку з метою підвищення пропускної здатності безпроводової мережі

Динамічна багатоадресна оптимізація (DMO) працює для максимально ефективної доставки багатоканальних кадрів. Багатоадресна передача вимагає, щоб контролер генерував кілька пакетів, по одному для кожної точки доступу і щоб безпроводові багатоадресні передачі відбувались із швидкістю передачі. Широкомовна та багатоадресна передача не підтверджуються (not acknowledged),

тому ці методи передачі використовують нижчі (повільніші) швидкості передачі даних, щоб забезпечити кращі шанси прийому.

Стандарт 802.11 стверджує, що багатоадресна передача через WLAN повинна передаватися з найнижчою підтримуваною швидкістю, щоб усі клієнти могли його декодувати. Низька швидкість передачі призводить до збільшення використання ефірного часу, а отже, і зниження загальної пропускної здатності передач. Через меншу швидкість бажано трансформувати багатоадресний трафік в одноадресний, коли кілька клієнтів підписалися на потік багатоадресної передачі. Трансформація багатоадресного трафіку до одноадресного збільшує швидкість безпроводової передачі, використовуючи вищі швидкості одноадресної передачі. На Рисунку 2.11 показано перехід DMO від багатоадресної до одноадресної передачі.

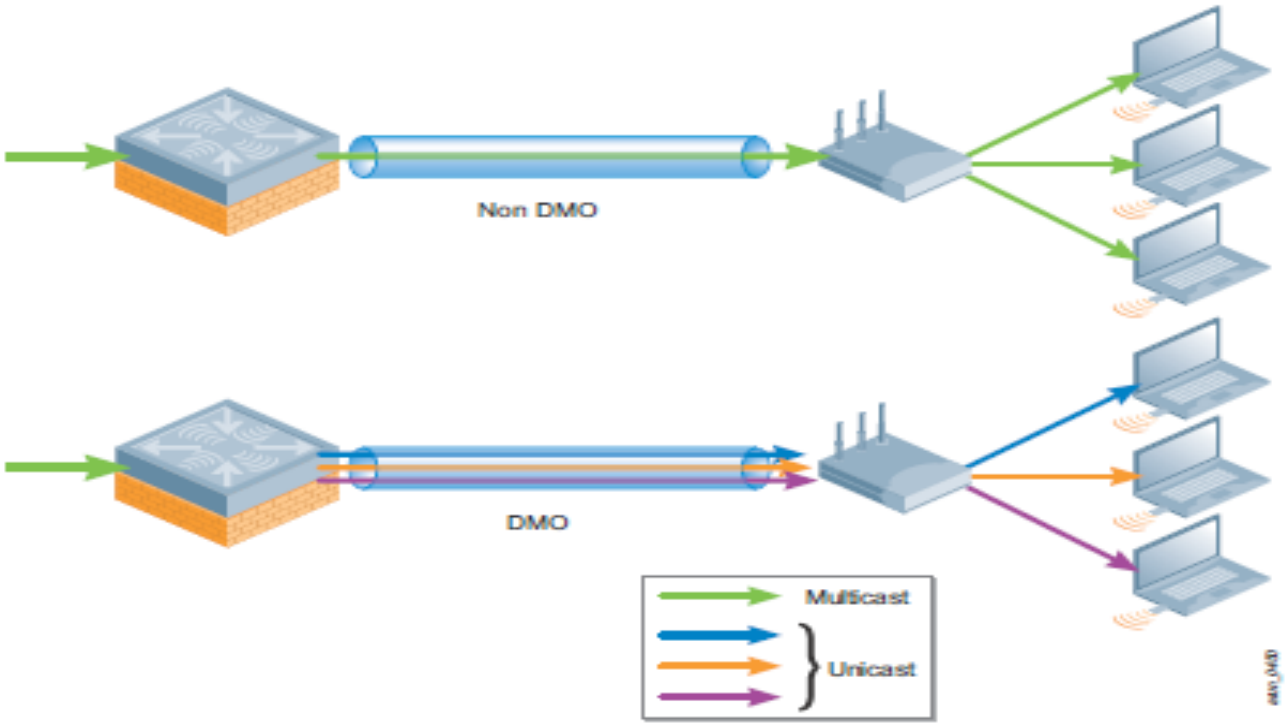

Рисунок 2.11 Конверсія багатоадресної передачі в одноадресну за допомогою DMO

Взагалі, одноадресний трафік може передаватися з більш високими швидкостями передачі і підтвердження забезпечує послідовну доставку. Однак після досягнення певної кількості клієнтів ефективніше повернутися до багатоадресних передач. DMO робить можливим надійну, якісну багатоадресну передачу через WLAN. Рішення Aruba підходить до проблеми надійності багатоадресної передачі на декількох фронтах:

IGMP Snooping і IGMP Proxy гарантують, що проводова інфраструктура надсилає багатоадресний трафік, наприклад, відеотрафік, лише тим точкам доступу, які мають активних абонентів;

DMO надсилає багатоадресний трафік як одноадресний, який може передаватися на набагато більших швидкостях та має механізм підтвердження для забезпечення надійної доставки багатоадресної передачі;

для DMO перетворення багатоадресного в одноадресне відбувається на контролері. Контролер пересилає одноадресні потоки підписаним клієнтам через відповідні точки доступу;

передача автоматично перемикається на багатоадресну передачу, коли кількість клієнтів збільшується настільки високо, що пропускна здатність каналу одноадресної передачі більше не може підтримуватися;

оптимізація швидкості багатоадресної передачі відстежує швидкості передачі, які є стабільними для кожного пов'язаного клієнта. Використовується найнижчий загальний стійкий тариф для багатоадресних передач для підписаних клієнтів, а не найнижчий рівень серед усіх клієнтів у цьому районі.

Як результат, надійне, високопродуктивне багатоадресне відео може передаватися через бездротову мережу високої щільності. Aruba рекомендує вмикати DMO лише в розгортаннях, де використовується багатоадресне відео. Порогове значення DMO слід встановити для 40 клієнтів або втричі більше кількості VLAN, залежно від того, що вище.

Функція розподіленої динамічної багатоадресної оптимізації (D-DMO) в ArubaOS 6.1.1 подібна до DMO, за винятком того, що перетворення багатоадресної передачі в одноадресну передачу відбувається в точці доступу замість контролера. DMO призначений для VAP в тунельному режимі переадресації, де перетворення багатоадресного в одноадресне відбувається на контролері. Для VAP, що працюють в режимі переадресації тунельного дешифрування, перетворення багатоадресного в одноадресне перенесення можна перемістити в точки доступу. Отже, VAP, які працюють у режимі переадресації тунельного дешифрування, застосовують DDMO замість DMO.

Споживання смуги пропускання на каналі між контролером і точками доступу є меншим з D-DMO, ніж DMO. Це пов’язано з тим, що в D-DMO передачі між контролером та точками доступу все ще залишаються багатоадресними, а фактичне перетворення багатоадресної передачі в одноадресну передачу відбувається лише на точці доступу. За допомогою D-DMO контролер надсилає

багатоадресні пакети в точки доступу лише через GRE-тунелі VAP-режимів дешифрування-тунелю, які мають активних абонентів. Кількість багатоадресних потоків через тунель GRE дешифрованого тунельного VAP на AP дорівнює сумі кількості груп багатоадресної передачі з активними абонентами на кожній VLAN на цій VAP. На малюнку 26 показаний перехід D-DMO від багатоадресного до одноадресного.

Споживання смуги пропускання на каналі між контролером і точками доступу є меншим, ніж D-DMO, ніж DMO. Це пов'язано з тим, що в D-DMO передачі між контролером та точками доступу все ще залишаються багатоадресними, а фактичне перетворення багатоадресної передачі в одноадресну передачу відбувається лише на точці доступу. За допомогою D-DMO контролер надсилає багатоадресні пакети в точки доступу лише через GRE-тунелі в режимі дешифрованого тунелю VAP, які мають активних абонентів. Кількість багатоадресних потоків через тунель GRE дешифрованого тунельного VAP на AP дорівнює сумі кількості груп багатоадресної передачі з активними абонентами на кожній VLAN на цій VAP. На Рисунку 2.12 показаний перехід D-DMO від багатоадресного до одноадресного.

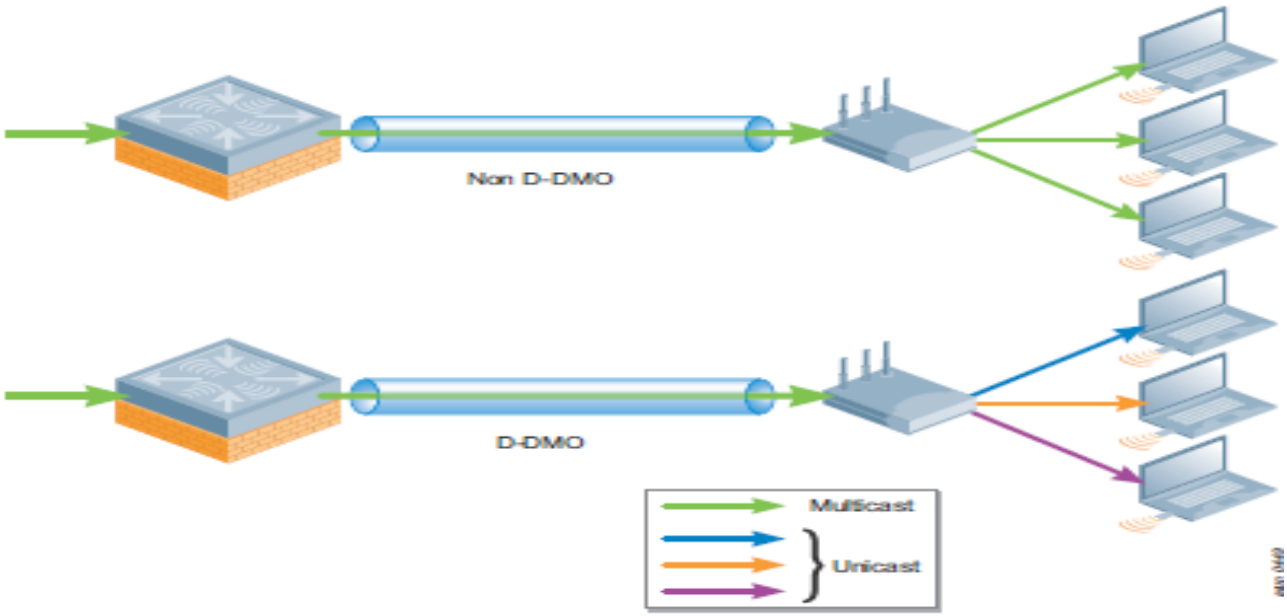

Рисунок 2.12 Конверсія багатоадресної передачі в одноадресну передачу за допомогою D-DMO

Коли ввімкнено проксі-сервер IGMP або відстеження, контролер має всю інформацію про активних абонентів багатоадресної розсилки на кожному BSSID кожного AP, що закінчується на цьому контролері. На основі цієї доступної інформації та визначеного порогового значення DMO контролер визначає, чи

повинна відбуватися перетворення багатоадресної передачі до одноадресної передачі, і якщо так, то для яких клієнтів, на яких BSSID. У D-DMO контролер надсилає рішення про перетворення багатоадресного в одноадресне передавання в точки доступу у вигляді растрового зображення разом із пакетом багатоадресної передачі. Точки доступу розглядають растрове зображення та виконують перетворення багатоадресної передачі в одноадресну передачу лише для тих клієнтів, зазначених у растровому зображенні. Коли бітова карта відсутня, точки доступу не виконують перетворення багатоадресної передачі в одноадресну передачу багатоадресного трафіку. Функції проксі-сервера IGMP та функції відслідковування IGMP на контролері забезпечують надсилання багатоадресного трафіку лише до точок доступу, які мають активних абонентів. Точки доступу ніколи не виконують відслідковування IGMP або проксі. Необхідно пам'ятати, що VAP повинні бути в дешифрованому тунельному режимі для роботи D-DMO.

В ArubaOS 6.1.1 D-DMO підтримується лише для VAPS для дешифрування тунелів на точках доступу в кампусі. Aruba рекомендує вмикати D-DMO лише в умовах розгортання багатоадресного відео, де політики мережі та безпеки дозволяють використовувати VAP-адреси дешифрування-тунелю. Поріг DMO слід встановити на рівні 40.

Пропускна здатність, яку споживають DMO та D-DMO в мережі між контролером та точкою доступу, залежить від різних факторів, таких як:

кількість абонентів багатоадресної передачі;

кількість активних груп багатоадресної розсилки;

кількість VLAN на VAP;

кількість VAP з підтримкою DMO або D-DMO на точці доступу.

Споживана смуга пропускання завжди пропорційна кількості потоків. Отже, різницю в смузі пропускання, споживану DMO та D-DMO, можна легко зрозуміти, обчисливши кількість потоків, що генеруються DMO та D-DMO за різних умов.

Кількість потоків між контролером та VAP для DMO можна розрахувати наступним чином:

Number of streams between the controller and a tunnel VAP for DMO	=	Number of active multicast subscribers on group 1	+	Number of active multicast subscribers on group 2	..... +	Number of active multicast subscribers on group n

Подібним чином кількість потоків між контролером та VAP дешифрувального тунелю для D-DMO можна обчислити наступним чином:

Number of streams between the controller and a decrypt-tunnel VAP for D-DMO	=	Number of active multicast groups on VLAN 1 of the VAP	+	Number of active multicast groups on VLAN 2 of the VAP	..... + Number of active multicast groups on VLAN n of the VAP

Таблиця підсумовує кількість потоків між контролером та одним VAP для DMO та D-DMO за різних умов.

Кількість активних абонентів у кожній групі багатоадресної розсилки			Активні групи багатоадресної розсилки у кожній VLAN на VAP			DMO (Number of streams between controller and a tunnel mode VAP)	DMO (Number of streams between controller and a decrypt-tunnel mode VAP)
Number of Subscribers on Multicast Group G1	Number of Subscribers on Multicast Group G2	Number of Subscribers on Multicast Group G3	Active Groups on VLAN 1	Active Groups on VLAN 2	Active Groups on VLAN 3		
1	1	1	G3	G1	G2	3	3
5	5	5	G2	G1	G3	15	3
5	5	5	G1, G2	G1, G3	G1, G2, G3	15	7
9	8	12	G2, G3	G3, G2, G1	G2	29	6
17	26	13	G1, G2, G3	G2,G3	G1, G2, G3	56	8

Стандарт 802.11 вимагає безпроводової багатоадресної передачі з базовою швидкістю передачі, щоб усі клієнти могли її декодувати. Низькі швидкості передачі вимагають більше ефірного часу, а також вони впливають на якість багатоадресного додатку в режимі реального часу, наприклад потокового відео. Одноадресний трафік може передаватися з більш високою швидкістю передачі до 450 Мбіт/с, тому DMO та D-DMO можуть забезпечити якіснішу багатоадресну передачу. Кількість потоків між контролером та VAP для чистої багатоадресної передачі (DMO та D-DMO вимкнено) однакова з D-DMO і менша, ніж DMO. Однак багатоадресний трафік завжди передається з дуже високою якістю, коли замість чистого багатоадресного передавання в ефірі використовуються DMO та D-DMO.

Справедливий доступ.

Wi-Fi використовує спільний носій інформації та використовується багатьма різними типами клієнтів та додатками. Отже, справедливий доступ до передачі даних стає надзвичайно важливим, особливо в часи високих суперечок між кількома клієнтами. По-перше, важливо, щоб усі клієнти отримали доступ до цього носія, коли вони мають дані для передачі. У той же час важливо також, щоб

нові, швидкісні клієнти могли скористатися цією швидкістю, не надто сповільнюючись старими клієнтами, які несправедливо витрачають ефірний час. Крім того, деякі передачі нетерпимі до затримки і вони повинні мати пріоритет перед передачею даних або фоновим трафіком.

Aruba використовує багатоступеневу систему класифікації для визначення класу трафіку та встановлення пріоритетів. Початковий вибір черги виконується брандмауером Aruba Policy Enforcement ™ (PEF ™) і його можна визначити різними способами, включаючи проводові флаги QoS, позначки WMM або відповідні правила брандмауера. Потім трафік формується на основі віртуальної точки доступу, що дозволяє чітко контролювати потоки руху.

Після того, як трафік класифікується та формується, він потрапляє в чергу на основі токенів. Залежно від пріоритету та доступності маркерів, кадри передаються в черги WMM для передачі. Система WMM має два однакові, але окремі набори черг: один для трафіку з високою пропускною здатністю (high throughput - HT) та інший для трафіку, що не є HT. Рисунок 2.13 зображує послідовність черги на Aruba.

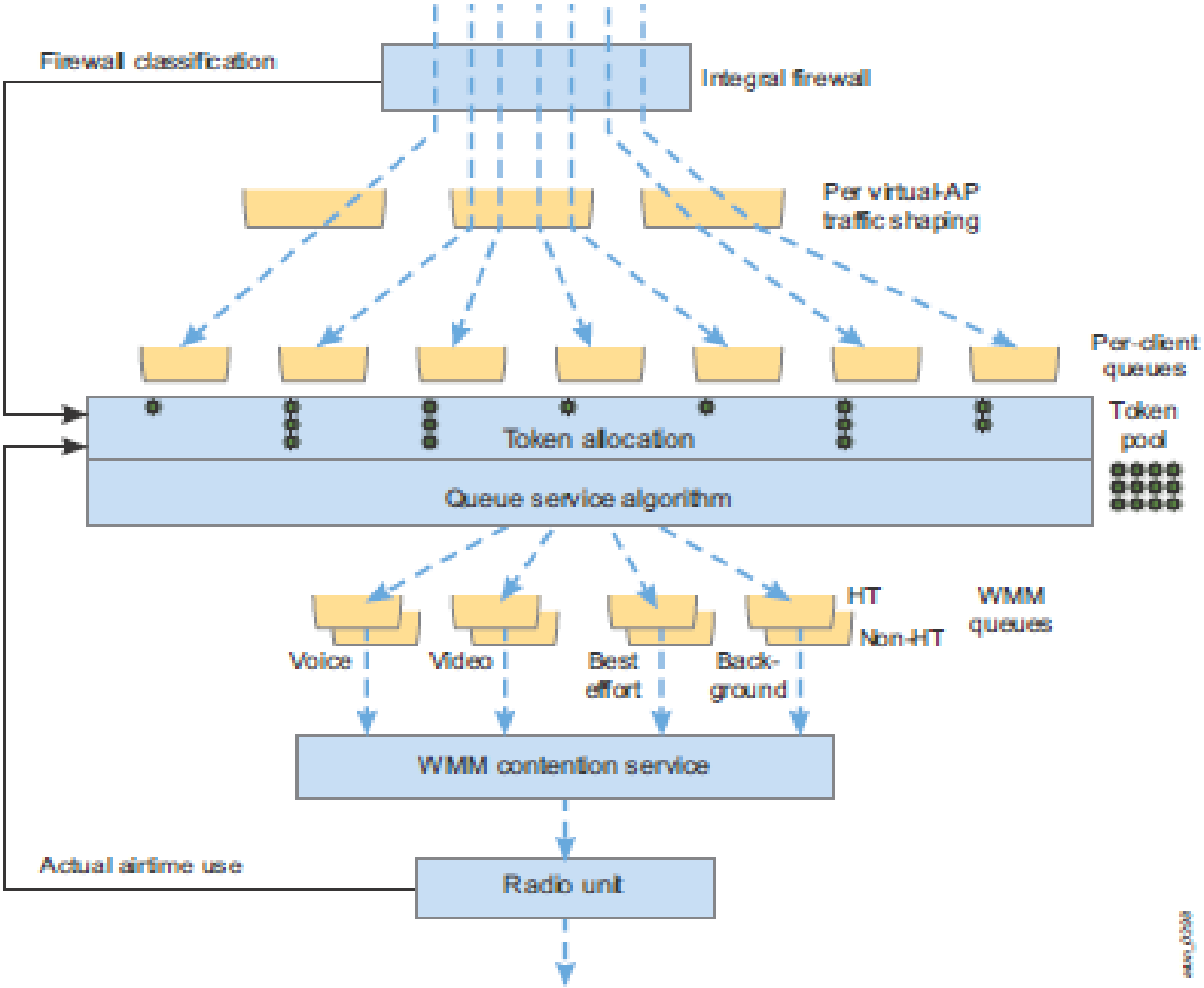

Рисунок 2.13. Послідовність черги в Aruba

Якість обслуговування (QoS) - це набір позначок пакетів та механізмів черги, які визначають пріоритети класів трафіку через мережу. Мультимедіа Wi-Fi (WMM) базується на поправці 802.11e. Це система для позначення трафіку як вищого пріоритету та регулювання таймерів пакетів, щоб дати чутливі до затримки дані мали перевагу в ефірі. Потоки, які зазвичай призначені для спеціальної обробки, включають голосові та відеопотоки, де потрібно контролювати пропускну здатність, втрату пакетів, тремтіння та затримку.

Зворотній зв'язок надходить від радіостанції до черги маркерів, щоб вплинути на обсяг трафіку, доступний клієнту. Голосовий та відеотрафік та підтвердження TCP також отримують особливий пріоритет. Що стосується голосового трафіку, система, по суті, скорочує черги та забезпечує суворий пріоритет. Для підтверджень TCP модуль PEF динамічно змінює розмір вікна TCP, щоб уповільнити відправника, де це необхідно, щоб уникнути заповнення черг.

Черга маркерів - це місце, де в системі забезпечується справедливість. Аруба пропонує три варіанти вирішення питання про порядок справедливості трафіку:

Доступ за замовчуванням: Цей параметр надає кожній черзі однакову вагу, як це було б для WMM AP без алгоритму ARM. Деякі ситуації можуть робити перевагу за замовчуванням, але це призводить до того, що менш спроможні клієнти отримують більше часу в ефірі, ніж швидші клієнти.

Справедливий доступ: Токени розподіляються на основі фактично використаного ефірного часу: клієнти, які використали більше ефірного часу, нещодавно отримують нижчий пріоритет для наступних передач. Ефект полягає у тому, щоб дозволити вищим режимам, таким як 802.11g проти b, надсилати більше трафіку за даний інтервал часу. Результат є "справедливим" в тому сенсі, що кожен клієнт отримує рівний час на спільному носії, незалежно від типу або можливості клієнта.

Бажаний доступ: Ця опція застосовує більші ваги до швидших режимів. Наприклад, цей параметр гарантує, що клієнту 802.11n, який може завершити передачу набагато швидше, ніж його еквівалент 802.11a, надається пріоритет у черзі. Преференційна справедливість пропонує найбільший загальний обсяг даних, але за певної вартості для менш спроможних клієнтів. Деякі менеджери

мереж використовують цю опцію як тонкий підштовх до популяції користувачів для оновлення до клієнтів 802.11n.

Aruba рекомендує забезпечити справедливий доступ для всіх розгортань для забезпечення якості обслуговування (QoS) та Wi-Fi мультимедіа (WMM).

2.5. Рекомендації щодо підвищення ефективності застосування Aruba Adaptive Radio Management (ARM)

Функція	**Розріджене розміщення AP лише з даними**	**Щільне розміщення AP лише з даними**	**При увімкненні відео**	**При увімкненні голосу**
Призначення ARM (ARM Assignment)	Односмугове сканування (за замовчуванням). Багатосмугове сканування (для AP з одним радіо)	Односмугове сканування (за замовчуванням). Багатосмугове сканування (для AP з одним радіо)	Односмугове сканування (за замовчуванням). Багатосмугове сканування (для AP з одним радіо)	Односмугове сканування (за замовчуванням). Багатосмугове сканування (для AP з одним радіо)
Клієнтський режим ARM (Client-Aware ARM).	Увімкнути	Увімкнути	Увімкнути	Увімкнути
Голосове сканування (Voice-Aware Scanning)	Увімкнути	Увімкнути	Увімкнути	Увімкнути
Відео сканування (Video-Aware Scanning)	Увімкнути	Увімкнути	Увімкнути	Увімкнути
Сканування з урахуванням навантаження (Load-Aware Scanning)	10 Мб/с (за замовчуванням)	10 Мб/с (за замовчуванням)	10 Мб/с (за замовчуванням)	10 Мб/с (за замовчуванням)
Енергозберігаюче сканування (Power-Save-Aware Scanning)	Вимкнути	Вимкнути	Вимкнути	Вимкнути
Сканування з урахуванням зловмисників (Rogue-Aware Scanning).	Вимкнути за винятком середовищ високого рівня безпеки	Вимкнути за винятком середовищ високого рівня безпеки	В Вимкнути за винятком середовищ високого рівня безпеки	Вимкнути за винятком середовищ високого рівня безпеки
Динамічний розподіл безпроводових клієнтів по діапазонах (Band Steering)	Увімкнути, віддати перевагу 5 ГГц (за замовчуванням)	Увімкнути, віддати перевагу 5 ГГц (за замовчуванням)	Увімкнути, віддати перевагу 5 ГГц (за замовчуванням)	Увімкнути, віддати перевагу 5 ГГц (за замовчуванням)

Функція	**Розріджене розміщення AP лише з даними**	**Щільне розміщення AP лише з даними**	**При увімкненні відео**	**При увімкненні голосу**
Балансування спектрального навантаження (Spectrum Load Balancing)	Вимкнути	Вимкнути	Вимкнути	Вимкнути
Режим ARM (Mode-Aware ARM)	Вимкнути	Вимкнути	Вимкнути	Увімкнути лише для вирішення проблем клієнта
Регулювання чутливості прийому (Adjusting Receive Sensitivity)	Вимкнути	Вимкнути	Вимкнути	Вимкнути
Місцевий поріг запиту зонда (Local Probe Request Threshold)	Вимкнути	Увімкнути (значення = 25 дБ)	Увімкнути (значення = 25 дБ)	Увімкнути (значення = 25 дБ)
Допомога при перемиканні станцій (Station Handoff Assist)	Вимкнути	Вимкнути	Вимкнути	Вимкнути
Інтелектуальна адаптація швидкості передачі (Intelligent Rate Adaptation)	Завжди включена, не налаштовується			
Динамічна багатоадресна оптимізація (Dynamic Multicast Optimization)	Вимкнути	Вимкнути	Вимкнути - вище 40 або 3-кратна кількість VLAN	Вимкнути
Справедливий доступ (Fair Access)	Увімкнути	Увімкнути	Увімкнути	Увімкнути

3 ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ НОВОГО УНІКАЛЬНОГО РІШЕННЯ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ ARUBA AIRMATCH ТА ARUBA CLIENTMATCH ДЛЯ ОПТИМІЗАЦІЇ РАДІОЧАСТОТНОГО РЕСУРСУ БЕЗПРОВОДОВОЇ МЕРЕЖІ

3.1 Налаштування та дослідження ефективності застосування рішення Aruba AirMatch

AirMatch - це послуга управління радіоресурсами наступного покоління, запроваджена в ArubaOS 8.0 для пристроїв із топологією Mobility Master/керованих пристроїв. AirMatch забезпечує безпрецедентну якість розподілу ресурсів мережі RF. Він аналізує статистику мережі RF за останні 24 години та попередньо оптимізує мережу на наступний день. Будь-яка зміна тарифного плану застосовується рано вранці, щоб мінімізувати порушення роботи клієнта та максимізувати взаємодію з користувачем. AirMatch може реагувати на шкідливі радіочастотні події, такі як радар та високий рівень шуму, щоб дозволити мережі керувати раптовими змінами в радіочастотному середовищі.

Aruba AirMatch виходить за рамки адаптивного управління радіо (ARM), використовуючи штучний інтелект та машинне навчання для забезпечення автоматизованої оптимізації радіочастот (RF). Замість того, щоб розглядати кожну окрему точку доступу, як у моделі ARM, AirMatch розглядає аналітику по всій WLAN.

Окремі контролери підтримують лише функції Adaptive Radio Management (ARM) та ClientMatch, які використовують автоматичні елементи керування на основі інфраструктури для максимізації продуктивності клієнта та підвищення стабільності та передбачуваності мережі Wi-Fi.

AirMatch та ARM не можна використовувати разом. ArubaOS 8.x не підтримує AirMatch на автономному контролері в режимі головного контролера. Розгортання Mobility Master, що включає керовані пристрої, не підтримує Adaptive Radio Management (ARM).

ArubaOS включає AirMatch та ClientMatch, унікальні можливості, які контролюють та оптимізують потужність Wi-Fi, канали, підключення та пропускну здатність по всій бездротовій мережі для поліпшення роботи користувачів.

AirMatch є ключовим компонентом бездротового рішення Aruba, що працює на основі штучного інтелекту і підтримується в середовищах, що використовують Aruba Mobility Conductor (ArubaOS 8+). Це забезпечує автоматизовану загальносистемну оптимізацію каналів, пропускну здатність та EIRP - не потрібно втручання вручну. Починаючи з ArubaOS 8.0 в Mobility Master - наступне покоління головного контролера - присвоєння статичних каналів у середовищах з високою щільністю зараз залишилось у минулому. За допомогою машинного навчання оптимальні канали, ширина каналу та призначення потужності виконуються повнстю автоматично, щоб максимізувати пропускну здатність у всій мережі Wi-Fi.

AirMatch аналізує періодичні радіочастотні дані по всій мережі або підмножині мережі (наприклад, кластер контролерів), щоб алгоритмічно отримувати зміни конфігурації для кожної точки доступу Aruba в мережі. Точки доступу регулярно оновлюються на основі змін умов навколишнього середовища, що приносить користь як IT, так і користувачам.

AirMatch поєднує в собі нові оптимізовані функції присвоєння каналу та потужності та додає функцію автоматичного регулювання ширини каналу, щоб забезпечити автоматизовану та динамічну оптимізацію RF для корпоративних WLAN. AirMatch призначений для галасливих середовищ із високою щільністю, де бракує чистого та невикористаного RF-спектру. Завдяки оптимальному призначенню каналу, ширини каналу та потужності передачі, AirMatch дозволяє:

рівномірний розподіл радіостанцій по доступних каналах, зменшення перешкод та максимальна пропускна спроможність системи;

динамічне регулювання пропускної здатності в діапазоні від 20 МГц, 40 МГц та 80 МГц відповідно до щільності вашого середовища;

найкраще покриття та навіть розподіл EIRP для безперебійного роумінгу.

Завдяки AirMatch підприємства можуть надавати кращу підтримку вимогливим та якісним чутливим програмам, таким як потокове передавання відео та Microsoft Skype for Business, перебуваючи в роумінгу по всьому підприємству.

Існуючі функції призначення каналів та потужності в ARM підтримують локальне сканування каналів, призначення каналів та регулювання потужності. Рішення приймаються локально в точці доступу, не враховуючи всю мережу. Завдяки динамічним методам машинного навчання AirMatch централізує цю функцію в Mobility Master, одночасно динамічно навчаючи мережу та адаптуючи

RF-планування для всієї мережі. Він не тільки розглядає окрему точку доступу, але й усю специфічну для радіочастотної інформації інформацію про точки доступу, таку як інтерференція, шум та радіолокаційні виявлення в мережі, до прийняття рішення. Оптимізований план радіочастот виводиться з однієї фази обчислень і конфігурація передається в точки доступу. Оптимізований радіочастотний план AirMatch призводить до довгострокової стабільності мережі з меншою кількістю необхідних змін каналів та потужності передачі при нормальних робочих умовах

Завдяки новій функції регулювання пропускної здатності каналу AirMatch автоматично налаштовує пропускну здатність каналу на основі щільності пристрою навколишнього середовища, максимізуючи пропускну здатність та покращуючи ефективність мережі.

Контролер Aruba Mobility Master збирає RF -статистику з усієї мережі. На основі даних за минулу добу AirMatch попередньо оптимізує план розподілу каналів для мережі, щоб забезпечити найвищу продуктивність. Крім того, точки доступу реагують на місцеві радіочастотні події, такі як високий рівень шуму та радіолокаційне виявлення, шляхом відповідної зміни каналів. Загалом, AirMatch забезпечує більш рівномірно розподілені канали в мережі із зменшеними перешкодами каналів та покращеним повторним використанням каналів. На Рисунку 3.1 показано призначення каналів за допомогою ARM. На Рисунку 3.2 показано більш рівномірний розподіл каналів за допомогою AirMatch на основі даних з усієї мережі.

Рисунок 3.1 Призначення каналу за допомогою ARM

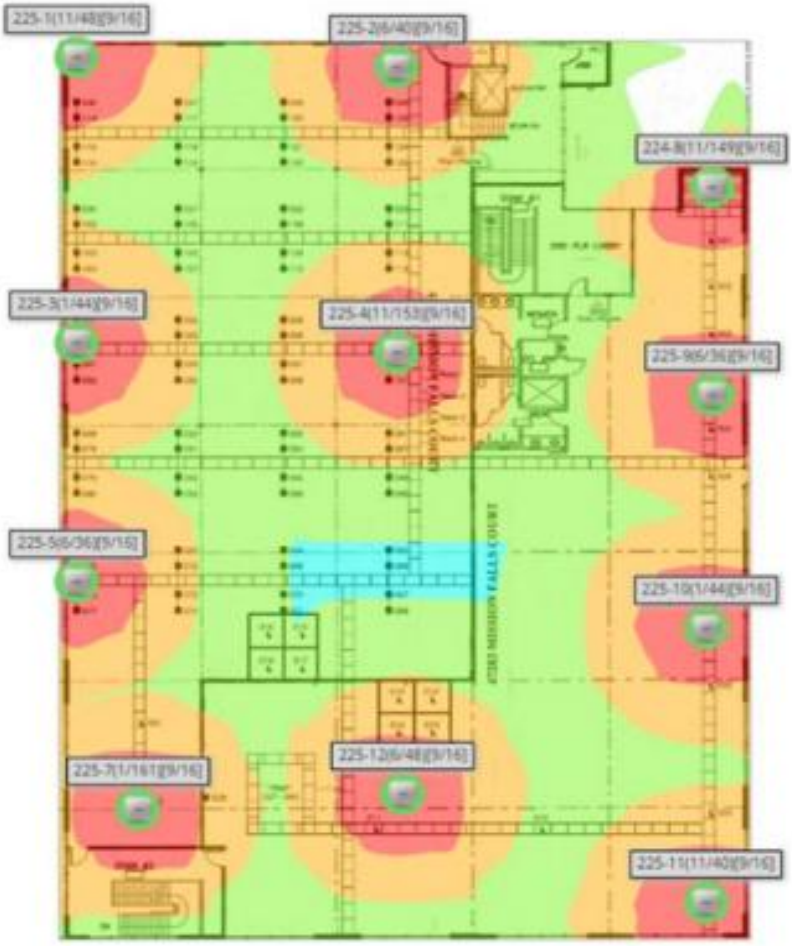

Рисунок 3.2 Призначення каналу за допомогою AirMatch

На Рисунку 3.1, як AP 225-3, так і AP 225-9 підтримують канал 1 на частоті 2,4 ГГц, а канал 149 на частоті 5 ГГц, що призводить до взаємного впливу каналів; в той час як на Рисунку 3.2, з AirMatch, канали як на радіостанціях 2,4 ГГц, так і на 5 ГГц розподілені більш рівномірно.

AirMatch перевіряє весь обсяг покриття WLAN і автоматично регулює потужність передачі точок доступу, щоб забезпечити найкраще покриття та зручність користування. Наприклад, коли AP не працює, це створює дірку покриття в мережі. AirMatch збільшить потужність передачі сусідніх точок доступу, щоб розширити покриття. Як показано на Рисунку 3.1 і Рисунку 3.2, щоб розширити покриття зазору в центрі прямокутної області, AirMatch відкоригував значення EIRP для всіх точок доступу навколо отвору до 9 дБм для 2,4 ГГц та 16 дБм для 5 ГГц симетрично; в той час як ARM коригував значення EIRP точок доступу асиметрично через локальний вигляд мережі.

Крім того, коли мережева інтерференція висока, AirMatch збільшить потужність передачі точок доступу, щоб пом'якшити інтерференцію каналу та покращити продуктивність WLAN. AirMatch також забезпечує мінімум диких коливань EIRP через сусідні точки доступу, що призводить до кращого досвіду роумінгу.

На додаток до оптимізованих функцій розподілу каналів та потужності, AirMatch розроблений з ще однією унікальною функцією - регулюванням пропускної здатності каналу. AirMatch розглядає щільність пристроїв у мережі та автоматично регулює ширину каналу радіо. Коли кількість підключених пристроїв збільшується, ширина каналу автоматично регулюється до більш вузького каналу, наприклад 40 МГц або 20 МГц, і навпаки. Для областей з дуже високою щільністю, таких як лекційні зали та стадіони, для кращої роботи рекомендується використовувати 20 МГц. Однак, якщо спочатку 20 МГц для мережі не планувалося, AirMatch автоматично перемкне смугу пропускання з 80 МГц або 40 МГц на 20 МГц на основі даних мережі в режимі реального часу. AirMatch переглядає загальну статистику мережі за останні 24 години та вносить поточні корективи. На Рисунку 3.3 показано регулювання ширини каналу на основі кількості пристроїв у середовищі з високою щільністю.

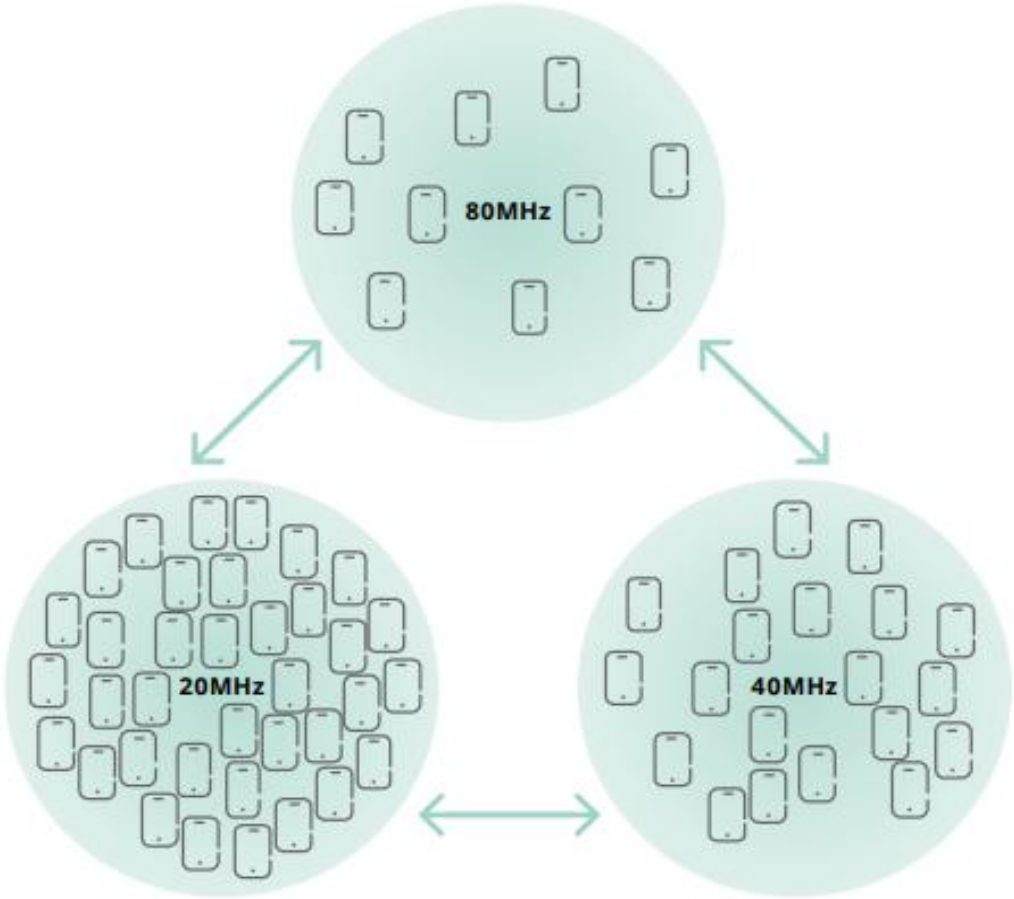

Рисунок 3.3 Регулювання ширини каналу за допомогою AirMatch в середовищах з високою щільністю

Для діапазону 5 ГГц у Північній Америці є загалом 6 каналів на 80 МГц, тоді як є 12 на 40 МГц і 25 на 20 МГц. На Рисунку 3.4 показано розподіл каналів FCC у Північній Америці. Завдяки більшій кількості каналів на частоті 20 МГц, планування каналів стає простішим, особливо в середовищах з високою щільністю.

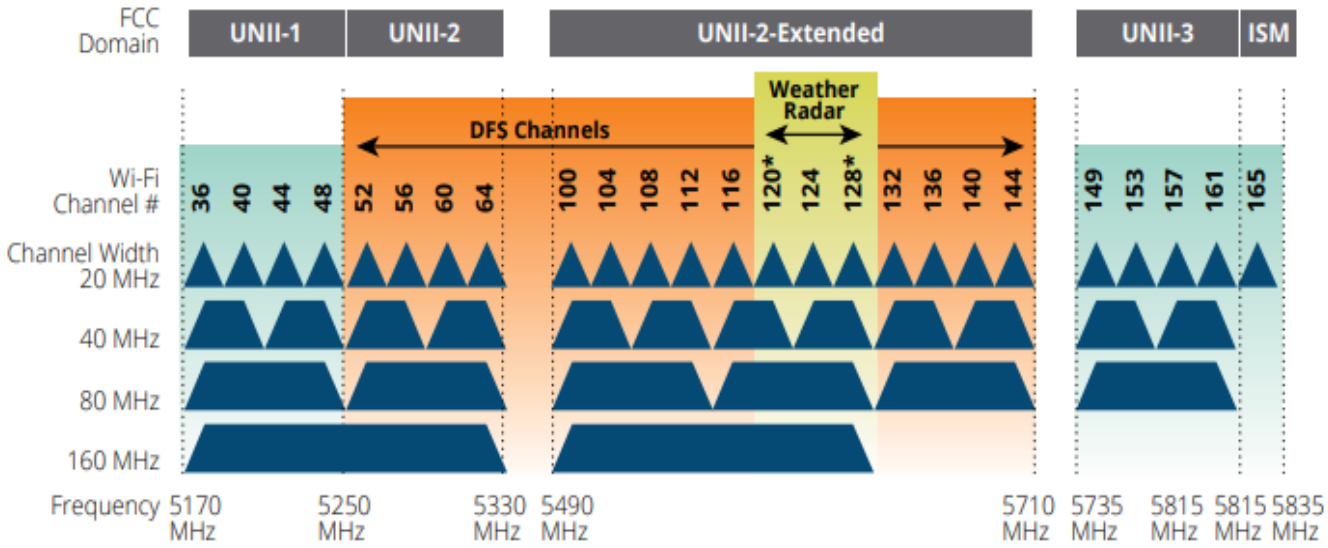

Рисунок 3.4 Розподіл каналів 5 ГГц у Північній Америці

Рівномірний розподіл EIRP по всіх точках доступу забезпечує кращий рівень покриття та ефективність роумінгу в сценаріях, коли спостерігаються радіочастотні події або прогалини покриття. У випадках високих мережевих перешкод через концентрацію клієнтів, радіолокаційні умови або інші джерела, AirMatch буде динамічно змінювати канали для пом’якшення ICH. Це також дозволить мінімізувати великі коливання EIRP на сусідніх точках доступу, щоб забезпечити безперебійну роботу користувачів.

Що стосується розривів покриття, на Рисунку 3.2 показано AirMatch, що поширює покриття на область блакитним кольором шляхом симетричного регулювання значень EIRP для всіх сусідніх точок доступу до 9 дБм в діапазоні 2,4 ГГц та 16 дБм в діапазоні 5 ГГц.

Призначення каналу AirMatch.

Кожен AP у розгортанні Mobility Master вимірює своє RF-середовище протягом п’яти хвилин, за замовчуванням кожні 30 хвилин. Потім точка доступу надсилає повідомлення AMON про можливість радіозв'язку на керований пристрій на основі апаратних можливостей цієї точки доступу, радіо- та регуляторного домену та RF сусідів. Керований пристрій пересилає ці повідомлення до Mobility Master. Mobility Master додає цю інформацію до бази даних, обчислює оптимальне рішення та розгортає найновіший RF-план, надсилаючи оновлені налаштування до точки доступу. За замовчуванням це оновлення конфігурації надсилається о 5 ранку (відповідно до системного годинника Mobility Master), але час цього оновлення конфігурації можна змінити за допомогою профілю AirMatch.

Винятком з цього щоденного оновлення є автоматична зміна каналу внаслідок події радіолокаційного виявлення або високої інтерференції. Якщо точка доступу виявляє радіолокаційну подію на поточному робочому каналі, вона автоматично переходить на інший підтримуваний канал, щоб уникнути радіолокаційних перешкод і не чекає щоденного оновлення конфігурації RF від Mobility Master. Точка доступу може також автоматично змінювати канали, якщо на поточному каналі виявлено дуже високий рівень шуму, якщо принаймні на одному іншому каналі немає шуму.

В ArubaOS 8.0 AirMatch переміщує радіостанцію на випадковий канал, коли виявляється радіолокаційна подія, або якщо на нестатичному каналі виявляється сильний шум. Починаючи з ArubaOS 8.0.1, AirMatch використовує критерії, описані в таблиці нижче, для призначення нового каналу.

Проблеми, що спонукають до зміни каналу	**Критерії вибору каналу**
Виявлений радар	AirMatch вибирає канал з мінімальним індексом перешкод з каналів без сильного шуму або радіолокаційного стану.
High channel noise	Критерії вибору каналів різняться між статичними та нестатичними каналами: якщо налаштований статичний канал, канал не змінюється через високий рівень шуму; для нестатичного каналу AirMatch вибирає канал з мінімальним індексом перешкод з каналів без сильних шумів або радіолокаційного стану.

Порогові значення якості каналу.

ArubaOS 8.0.1 вводить поріг покращення якості каналу AirMatch, що дозволяє вибрати мінімальне вдосконалення каналу, яке може викликати нове заплановане рішення каналу. Порогове значення за замовчуванням - це покращення на 15%. Якщо запропонована зміна каналу не призведе до покращення, яке відповідає або перевищує цей поріг, AirMatch не ініціює зміну каналу.

Цей параметр якості каналу застосовується лише до запланованих оновлень. Якщо ви вручну активуєте оновлення за допомогою команди *airmatch runnow*, AirMatch розгорне нове рішення незалежно від рівня значення якості каналу.

Початкові RF розрахунки.

База даних служби AirMatch порожня, коли Mobility Master вперше завантажився. Коли Mobility Master вперше виявляє точки доступу в мережі, він переходить до початкової фази оптимізації, збирає дані з усіх точок доступу та генерує додаткове рішення кожні 30 хвилин (за замовчуванням) протягом наступних восьми годин. По закінченню цього початкового восьмигодинного періоду служба AirMatch періодично обчислює нову RF конфігурацію для цих пристроїв.

Коли новий AP розгортається в мережі з активним Mobility Master під час початкової 8-годинної фази оптимізації AirMatch, цей AP приєднується до мережі зі своїми попередньо призначеними значеннями каналу та потужності передачі. Служба AirMatch виявляє нещодавно розгорнуту точку доступу в мережі, перезапускає свої обчислення RF і надсилає поступове оновлення RF конфігурації до нової точки доступу через 30 хвилин. Точки доступу, додані в мережу після початкового 8-годинного періоду оптимізації, не отримають додаткового оновлення RF конфігурації до наступного запланованого періоду оновлення.

Налаштування AirMatch.

Діапазон RF налаштувань, які можна призначити точці доступу за допомогою функції AirMatch, визначений у радіопрофілях 2,4 ГГц та 5 ГГц на керованому пристрої. Можна отримати доступ до цих налаштувань на Mobility Master WebUI, вибравши конфігурацію керованого пристрою з ієрархії конфігурації, а потім перейшовши до *Configuration > AP Groups > Radio and Configuration > Access Points > Radio pages*. Можна використати ці сторінки, щоб вказати режим радіо, діапазон каналів та максимальну пропускну здатність каналів, яку можна призначити точці доступу або групі точок доступу за допомогою рішення AirMatch. Функція AirMatch не призначить точці доступу канал, який не входить до групи дійсних каналів або діапазонів смуги пропускання каналів, дозволених радіопрофілем 2,4 та 5 ГГц цієї точки доступу.

Функція AirMatch виконує автоматичні щоденні оновлення за замовчуванням, але можна використовувати веб-інтерфейс Mobility Master WebUI або інтерфейс командного рядка, щоб вимкнути щоденні оновлення для точок доступу в одному або декількох вузлах конфігурації, дозволяючи цим точкам доступу зберегти свою існуючу конфігурацію RF. Якщо оновлення AirMatch змінено з налаштування за замовчуванням на вимкнене, Mobility Master продовжує отримувати RF оновлення від AP, але Mobility Master не виконує жодних змін каналу або EIRP.

Налаштування відключеного AirMatch відрізняється від налаштування вимкнення або підтримання ARM на автономному контролері. Параметр вимкнення ARM змінює канал каналу радіостанції та значення EIRP назад до значень за замовчуванням, зазначених у радіопрофілях 802.11a та 802.11g радіостанції AP. Налаштування підтримки ARM заморожує поточний канал радіо та налаштування EIRP. На відміну від цього, якщо ви використовуєте AirMatch у топології Mobility Master/Managed Device, відключена опція AirMatch просто означає, що централізований алгоритм припинить вибір нового каналу, смуги пропускання або налаштування EIRP; оператор мережі все ще може замінити попередні налаштування, призначені AirMatch, статичними значеннями каналів або EIRP, а радіостанція AP може продовжувати добровільно змінювати канали, щоб уникнути інтерференції з радаром або високого рівня шуму.

Можна використовувати WebUI або інтерфейс командного рядка (CLI - Command Line Interface) для визначення найбільш часто використовуваних параметрів конфігурації AirMatch, але деякі розширені налаштування AirMatch доступні лише через CLI.

Налаштування AirMatch за допомогою WebUI.

Щоб зберегти існуючу конфігурацію AirMatch RF і вимкнути майбутні оновлення в ArubaOS 8.0.1 або новішої версії необхідно:

в ієрархії вузла *Mobility Master*, перейдіть до *Configuration* > *Services* > *AirMatch*;

зніміть прапорець біля пункту *Automatically deploy RF plan*;

клікніть *Submit*;

виберіть *Pending* Changes;

у вікні *Pending Changes*, встановіть прапорець і натисніть *Deploy changes*.

Для зміни часу щоденних оновлень AirMatch RF необхідно:

в ієрархії вузла *Mobility Master*, перейдіть до *Configuration* > *Services* > *AirMatch*;

у полі *Activation Time*, введіть число від 0 до 23, щоб вказати годину оновлення (у 24-годинному форматі);

клікніть *Submit*;

виберіть *Pending Changes*;

у вікні *Pending Changes*, встановіть прапорець і натисніть *Deploy changes*.

Налаштування AirMatch за допомогою CLI.

Щоб зберегти існуючу конфігурацію AirMatch RF необхідно:

(host) [mynode] (config) #airmatch profile schedule disable

Щоб змінити час щоденних оновлень AirMatch RF з типових 5:00 на 02:00:

host) [mynode] (config) #airmatch profile deploy-hour 2

Використовуйте параметр порогу якості (quality-threshold), щоб змінити відсоток поліпшення якості каналу, що спричинить заплановане оновлення AirMatch RF. Якщо запропонована зміна каналу не призведе до покращення, яке відповідає або перевищує цей поріг, AirMatch не ініціює зміну каналу.

(host) [mynode] (config) #airmatch profile quality-threshold <quality-threshold>

Використовуйте інтерфейс командного рядка Mobility Master, щоб вручну ініціювати обчислення AirMatch RF та розгортання рішення, а не чекати наступного запланованого періоду оновлення. Зайдіть на інтерфейс командного рядка в режимі ввімкнення та видайте таку команду:

(host) [mynode] #airmatch runnow full

Команда *airmatch ap freeze* розгортає вказаний канал та значення EIRP на радіо одразу, а потім заморожує ці значення, незалежно від того, чи встановлено функцію планування AirMatch RF для ввімкнення чи вимкнення режиму. Радіоприймач із командою *airmatch ap freeze* використовує статичну конфігурацію радіо, поки ці налаштування явно не скасовуються командою *airmatch ap unfreeze*. За допомогою цієї команди можна заморозити або канал, або значення EIRP, або обидва значення. Наприклад, ви можете заморозити канал на радіостанції точки доступу, дозволяючи при цьому AirMatch оновлювати значення EIRP.

(host)[mynode](config)# airmatch ap freeze {ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}|{ap-name<ap-name>}|{ap-group <ap-group>}|{all-aps} {band <band>}|{channel <channel>}|{eirp <eirp>}{lms{lms-ip <lms-ip>}|{{lms-ipv6 <lms-ipv6>}}

Розморожування конфігурації радіо за допомогою команди *airmatch ap unfreeze* не означає, що автоматично відбудеться негайна зміна значень каналу радіо та значення EIRP. Однак це означає, що алгоритм AirMatch може призначити новий набір значень під час наступного оновлення.

(host)[mynode](config)# airmatch ap unfreeze {ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}|{apname <ap-name>}|{ap-group <ap-group>}|{all-aps} band <band> {channel <channel>}|{eirp <eirp>}{lms{lms-ip <lms-ip>}|{{lms-ipv6 <lms-ipv6>}}

За замовчуванням кожна точка доступу в розгортанні Mobility Master вимірює своє RF-середовище протягом п’яти хвилин, за замовчуванням кожні 30 хвилин. Mobility Master використовує цю інформацію для обчислення оптимального рішення, а потім розгортає найновіший RF-план, надсилаючи оновлені налаштування в точки доступу. Використовуйте команду *ap system*

profile, щоб змінити ці інтервали звітів за замовчуванням або вимкнути звіти AirMatch для точок доступу.

(host) [mynode] (config) #ap system-profile <profile>
airmatch-measure-duration <airmatch-measure-duration>
airmatch-report-enabled
airmatch-report-period <airmatch-report-period>

3.2 Налаштування та дослідження ефективності застосування рішення Aruba ClientMatch

Забезпечення того, щоб усі клієнти безпроводової мережі отримували відповідні рівні обслуговування, є основною проблемою, особливо коли телефони, планшети та інші мобільні пристрої вибирають, до яких доступних SSID-кодів підключатись, незалежно від стану мережі. Це може суттєво вплинути на ефективність роботи клієнта, а також загальний стан роботи мережі. Проблеми можуть виникати у клієнтів, які з'єднуються зі слабкими сигналами, підключаються до закріпленої точки підписки (AP), а також від клієнтів, які вперто залишаються підключеними до однієї точки доступу, навіть коли вони пересувається в зону з точками доступу, що забезпечує кращі зв'язки.

Щоб вирішити ці проблеми, Aruba вдосконалює традиційні радіо- та роумінгові методи (наприклад, діапазон управління та 802.11k/v/r) завдяки введенню ClientMatch. Ця запатентована технологія радіочастотної оптимізації на точках доступу Aruba значно підвищує продуктивність клієнта та забезпечує передбачуваний і послідовний досвід підключення по всій безпроводовій локальній мережі (WLAN). Як частина рішення Aruba Mobility Mobility, ClientMatch постійно контролює стан усіх клієнтів, підключених до кожної точки доступу, та інтелектуально групує клієнтів до точок доступу, оптимізованих для перенесення їхнього трафіку - не потрібне спеціалізоване клієнтське програмне забезпечення (Рисунок 3.5). Як результат, вплив клієнтів на продуктивність загальної мережі WLAN різко знижується.

Ключовими характеристиками ClientMatch є наступні:

вирішує проблеми з липкими клієнтами та покращує продуктивність клієнтів Wi-Fi 6 та Wi-Fi 5;

бере участь у рішенні про рухливість на основі штучного інтелекту на Aruba;

постійно оптимізує підключення клієнта, щоб загальна продуктивність мережі залишалася незмінною;

зворотна сумісність для всіх клієнтів 802.11a/b/g/n/ac - додаткове програмне забезпечення не потрібне.

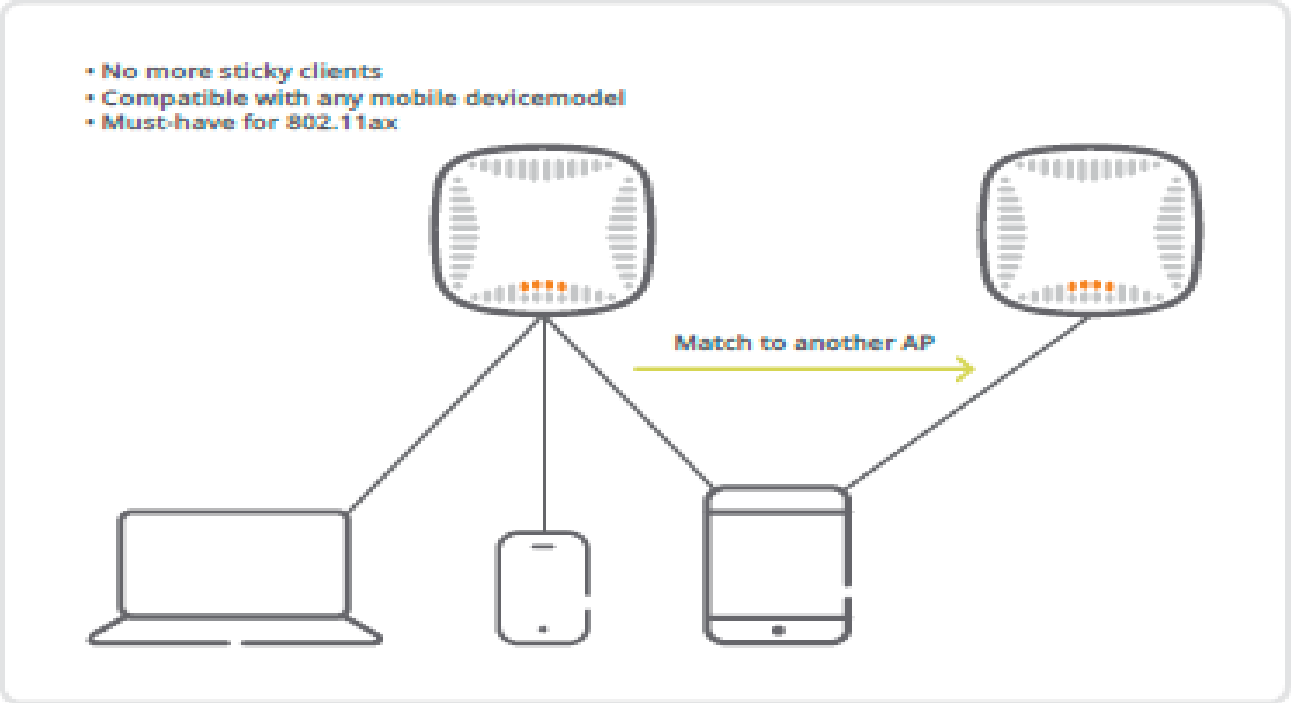

Рисунок 3.5 Технологія ClientMatch усуває проблеми з липким клієнтом для будь-якого мобільного пристрою

Характеристики, що використовуються для поліпшення якості мережі, включають: підтримувані стандарти Wi-Fi (наприклад, Wi-Fi 6, Wi-Fi 5), можливості MU-MIMO, доступні радіостанції, швидкість проти діапазону та інші атрибути рівня системи.

Останній стандарт Wi-Fi забезпечує підвищену продуктивність, швидкість та ефективність завдяки таким функціям, як OFDMA, 1024-QAM та двонаправлений MU-MIMO. Але ці можливості неможливо реалізувати в повному обсязі, якщо клієнти, які не мають Wi-Fi 6 (наприклад, датчик 802.11n або принтер 802.11ac), мають однакову точку доступу з клієнтами Wi-Fi 6. Для вирішення цього питання ClientMatch було вдосконалено завдяки обізнаності з Wi-Fi 6, що дозволяє згрупувати клієнтів Wi-Fi 6, щоб повною мірою скористатися перевагами багатокористувацьких функцій Wi-Fi 6. Крім того, ClientMatch також покращує досвід клієнтів Wi-Fi 5 із підтримкою MU-MIMO, також групуючи їх для реалізації розширених переваг.

Поведінка клієнта відіграє значну роль у роботі WLAN. Фактори включають:

Прийняття рішень на основі клієнта.

Клієнти, як правило, контролюють рішення щодо підключення, наприклад, до якої точки доступу приєднатись, швидкість передачі даних та роумінг. Оскільки їм бракує подання на системному рівні, клієнти в переповненому середовищі все одно можуть підключатися до перевантаженого діапазону 2,4 ГГц, навіть коли доступний чистіший діапазон 5 ГГц, що суттєво впливає на роботу клієнта та загальну продуктивність.

Непередбачувана продуктивність.

Погана продуктивність клієнта безпосередньо впливає на досвід користувачів і може призвести до зростання витрат на підтримку. IT часто виділяють ресурси для управління довідковою службою та усунення несправностей у мережі при повільній продуктивності Wi-Fi або з'єднанні.

Різноманітність клієнтів.

Зі зростанням кількості та типу мобільних клієнтів та клієнтів IoT, що отримують доступ до додатків, що вимагають пропускної здатності, ефірний час стає все більш цінним. Величезна кількість та різноманітність клієнтів впливає на ефективність роботи, оскільки повільні клієнти перешкоджають усім іншим клієнтам. Щоб проілюструвати це, якщо Клієнт 1, планшет 802.11g зі швидкістю 54 Мбіт/с отримує доступ до Dropbox на AP 1, то Клієнт 2, ноутбук Wi-Fi 6, здатний до 3,5 Гбіт/с, повинен зачекати в черзі перед тим, як зв’язатись з тією самою AP 1.

Клієнти підключаються до AP на основі сигналу, а не завантаження.

На додаток до липких проблем з клієнтами, пристрої зазвичай підключаються до найсильнішої точки доступу, яку вони чують, навіть якщо на точці доступу перевищена кількість користувачів (наприклад, у зайнятому фойє, аудиторії, лекційному залі тощо), створюючи дисбаланс у використанні мережі.

ClientMatch відрізняється тим, що він використовує системний підхід до усієї мережі для постійного моніторингу стану всіх пов'язаних клієнтів. Динамічно збираючи інформацію про клієнта (наприклад, потужність сигналу та використання каналу) з кожної точки доступу без будь-якого клієнтського програмного забезпечення для встановлення або обслуговування, його легко впровадити в масштабі. Потім ці дані клієнта агрегуються та передаються між

усіма точками доступу для координації та прийняття рішень у режимі реального часу, коли умови змінюються.

Наприклад, ClientMatch визначає, коли клієнт підключений до точки доступу, на якій перевищена кількість користувачів та коли існує точка доступу з меншим перевантаженням із сильнішим сигналом, шо знаходиться лише на відстані 15 футів. Потім він буде динамічно переміщувати клієнтів відповідним чином.

ClientMatch включає вбудовану інформацію про активні відео- та голосові сесії. Це означає, що клієнти, які заангажовані у Skype for Business, залишатимуться на зв'язку, щоб мінімізувати порушення роботи користувача.

Дводіапазонні клієнти будуть перенесені з радіостанції 2,4 ГГц на доступну радіостанцію 5 ГГц, яка має добрий або відмінний рівень сигналу, щоб покращити для клієнта кількість доступних каналів, відношення сигнал/шум (SNR), пропускну здатність (наприклад, можливість використання ширших каналів).

Ефективність клієнта та точки доступу постійно контролюється, щоб забезпечити найкращий досвід роботи з клієнтом. Клієнти віддаляються від неоптимальних точок доступу під час спроб підключення та коли стан здоров'я клієнта погіршується. Наприклад, клієнт, який підключається до точки доступу зі слабким сигналом, буде переміщений до більш підходящої точки доступу (Рисунок 3.6), а клієнт, який залишається підключеним до точки доступу, коли він від неї віддаляється (проблема з липким клієнтом) також буде переміщений до найближчої AP з кращою ефективністю (Рис 3.7).

Рисунок 3.6 План показує проблемного клієнта (червоний), який ClientMatch автоматично спрямовує до кращої точки доступу

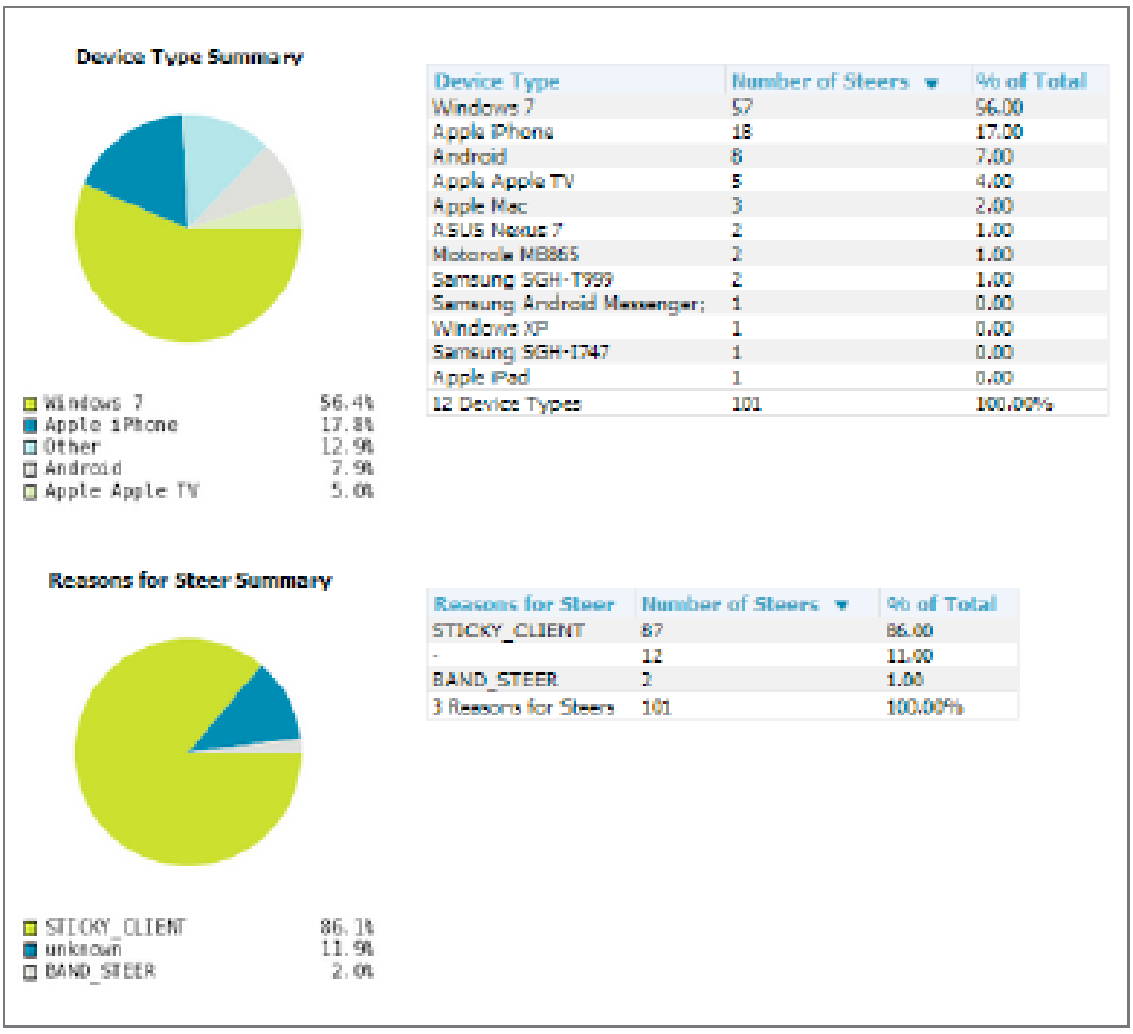

Рисунок 3.7 Звіт ClientMatch, який показує липких клієнтів, якими керували, скільки разів вони були під керуванням та причина керування ними.

ClientMatch постійно здійснює моніторинг RF-району клієнта, щоб забезпечити постійне керування діапазоном клієнтів та балансування навантаження, а також перепризначенням точки доступу для мобільних клієнтів у роумінгу.

Керований пристрій агрегує інформацію, яку отримує з усіх точок доступу, використовуючи ClientMatch і зберігає інформацію для всіх пов'язаних клієнтів у базі даних. Керований пристрій надає цю базу даних точкам доступу (для пов'язаних з ними клієнтів), а точки доступу використовують інформацію для обчислення клієнтського району RF і визначають, які точки доступу слід розглядати як точки доступу для кожного клієнта. Коли керований пристрій отримує запит на керування клієнтом від точки доступу, керований пристрій визначає оптимального кандидата AP і керує переміщенням клієнта на бажану радіостанцію. Це є покращенням порівняно з попередніми випусками, де ARM

управляли виключно точками доступу, без більшої перспективи для RF оточення клієнта.

У розгортаннях Mobility Master/керованих пристроїв, де точки доступу підключені до керованого пристрою, який пов'язаний з Mobility Master, AP надсилає інформацію про RF оточення на керований пристрій, який потім пересилає цю інформацію до Mobility Master. Mobility Master отримує звіти про зондування з усіх керованих пристроїв та генерує Virtual Beacon Report (VBR) для кожного клієнта. Ці VBR надсилаються від Mobility Master до керованого пристрою, а потім до точки доступу, до якої прив'язаний клієнт. Точки доступу, пов’язані з автономним контролером, отримують та збирають інформацію про клієнтів, що знаходяться в їх сусідстві і періодично надсилають цю інформацію контролеру, який, у свою чергу, генерує VBR і відправляє їх безпосередньо назад до AP.

Правила ClientMatch, які керують асоціаціями клієнтів, базуються, головним чином, на RF-середовищі клієнта і застосовуються однаково до всіх типів клієнтів, незалежно від типу пристрою чи операційної системи. ArubaOS 8.0 підтримує поступові оновлення правил ClientMatch для підтримки мережевих пристроїв, що працюють на новіших операційних системах, які можуть бути несумісні з існуючими правилами асоціації клієнта ClientMatch. Ця функція дозволяє керованому пристрою використовувати новіший набір правил ClientMatch без оновлення всієї операційної системи, зменшуючи час простою мережі.

ClientMatch пропонує більш тісну інтеграцію з безліччю підтримуючих медіа ALG, щоб забезпечити кращу якість дзвінків для таких програм, як Skype for Business (Skype4b) та Facetime. Завдяки можливості ClientMatch розуміти різні мультимедійні протоколи, клієнти не перенаправляються на різні точки доступу в середині активного медіа-сеансу.

Коли клієнт бере участь у дзвінку, керований пристрій дізнається про сеанс мультимедіа та надсилає цю інформацію до точки доступу, до якої в даний момент приєднаний клієнт, як частина оновлення змінної бітрейту (VBR). Коли точка доступу дізнається, що клієнт здійснює дзвінок, вона не намагатиметься перенаправити клієнта на іншу точку доступу, поки керований пристрій не вкаже, що виклик закінчився, дозволяючи дзвінкам проходити плавніше без будь-яких порушень поточного медіа-потоку.

Багатокористувацьке керування MIMO, або MU-MIMO, групує багатокористувацьких (MU-здатних) клієнтів, щоб максимізувати ймовірність передачі MIMO, що підвищує пропускну здатність низхідного потоку в точках доступу 802.11ac Wave 2 (gen 2). MU-MIMO працює на клієнтах, що підтримують MU, з потоками трафіку та PHY-каналами, сумісними для багатокористувацьких передач. ClientMatch керує та вирівнює клієнтів, що підтримують MU-MIMO, та радіостанції, що підтримують MU-MIMO, використовуючи значення SNR. Кілька клієнтів, що підтримують MU-MIMO, можна згрупувати за допомогою радіостанції, що підтримує MU-MIMO.

Налаштування ClientMatch.

Необхідно використовувати наступні процедури, щоб вимкнути або ввімкнути ClientMatch та завантажити пакет оновления Rules-Based ClientMatch (RCBM).

ClientMatch увімкнено за замовчуванням. Процедура вимкнення та повторного ввімкнення ClientMatch варіюється залежно від того, чи складається розгортання з декількох керованих пристроїв, якими керує Mobility Master, чи всі точки доступу пов’язані з автономним контролером.

Розгортання Mobility Master.

ClientMatch увімкнено та вимкнено в налаштуваннях радіостанцій 2,4 ГГц та 5 ГГц групи AP:

в ієрархії вузла *Managed Network* перейдіть на сторінку *Configuration > AP Groups;*

виберіть ім'я групи точок доступу з таблиці *AP Groups*;

клікніть на вкладку *Radio* під таблицею *AP Groups*, щоб відобразити налаштування радіо точки доступу;

розгорніть розділ *Client Control;*

клікніть *Client-Match* на випадачому списку для радіостанцій 2,4 ГГц і 5 ГГц, щоб увімкнути або вимкнути ClientMatch для цих радіостанцій;

змініть потрібні налаштування та клікніть *Submit*;

клікніть *Pending Changes*;

у вікні *Pending Changes* клікніть *Deploy Changes*.

Автономні розгортання Контролерів.

Для автономних контролерів, які не мають жодних пов’язаних керованих пристроїв, функція ClientMatch увімкнена та вимкнена в профілі адаптивного управління радіо (ARM) точки доступу. Хоча налаштування по замовчуванню

ClientMatch для більшості користувачів, розширені налаштування ClientMatch можна налаштувати за допомогою команд *rf arm-profile* в інтерфейсі командного рядка.

Використовуйте WebUI або інтерфейс командного рядка, щоб завантажити власний файл оновлення правил ClientMatch до папки */flash/config* на Mobility Master. Ця функція недоступна для розгортання окремих контролерів.

Налаштування AirMatch за допомогою WebUI.

Щоб завантажити пакет оновлення правил ClientMatch в ArubaOS 8.0.1 або новішої версії необхідно:

у ієрархії вузла *Mobility Master* перейдіть до *Diagnostics > Technical Support > Client Match Rules*;

клікніть *Upload File*, а потім виберіть файл для завантаження;

клікніть *Submit*;

клікніть *Pending Changes*;

у вікні *Pending Changes* клікніть *Deploy Changes.*

Налаштування AirMatch за допомогою інтерфейсу командного рядка CLI.

(host) [mynode] (config) #copy tftp: <tftphost> <filename> flash: <destname>

(host) [mynode] (config) #copy ftp: <ftphost> <user> <password> flash: <destname>

(host) [mynode] (config) #copy scp: <scphost> <username> <password> flash: <destname>

ВИСНОВОК

1. Інтерференція в мережі WLAN 802.11 є як неминучим, так і непередбачуваним явищем. Тому цим явищем потрібно керувати, щоб забезпечити надійну роботу мережі Wi-Fi, що вимагає інтегрованого набору функцій, які постійно контролюють радіочастотне середовище та оптимізують радіочастотну систему. Технологія адаптивного радіозв'язку (Adaptive Radio Management - ARM), яка контролює якість каналів безпроводових мереж Aruba, підвищує надійність та продуктивність, використовуючи засоби керування на основі інфраструктури для підвищення загальної продуктивності мережі на основі адаптивного радіочастотного сканування на всіх точках доступу Aruba, що гарантує обізнаність контролера безпроводової мережі про миттєву інтерференцію та індекси покриття. В той же час, робота системи ARM не є повністю автоматизованою. Для забезпечення найбільшої ефективності функціонування безпроводової мережі необхідно здійснити оптимізацію використання радіочастотного ресурсу, що досягається ефективним застосуванням інтегрованого набору функцій ARM.

2. На базовому рівні Aruba Adaptive Radio Management (ARM) дозволяє мережі враховувати Wi-Fi і не Wi-Fi інтерференцію та інші AP, для налаштовування параметрів каналів точок доступу. AP та SM постійно сканують навколишнє середовище. Якщо в мережі з’являється заважаючий пристрій (Wi-Fi або не Wi-Fi), який подавляє канал, ARM належним чином налаштовує канали AP. Якщо точка доступу виходить із ладу, ARM автоматично заповнює діру радіочастотного покриття, збільшуючи потужність навколишніх точок доступу.

В той же час, для оптимізації радіочастотного ресурсу на базі програмно-апаратного комплексу Aruba Adaptive Radio Management (ARM) необхідно ретельно виконувати рекомендації щодо підвищення ефективності застосування ARM шляхом оптимального вибору, наприклад, таких функцій, як: увімкнення клієнтського, відео та голосового сканування; увімкнення динамічного розподілу безпроводових клієнтів по діапазонах; вимкнення механізму регулювання чутливості прийому точок доступу у щільному розгортанні; увімкнення механізму інтелектуальної адаптація швидкості передачі; увімкнення механізму справедливого доступу до передачі даних.

3. Подальше підвищення ефективності оптимізації радіочастотного ресурсу можливе за рахунок застосування унікального рішення Aruba AirMatch, побудованого на використанні штучного інтелекту та машинного навчання.