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 ЕФЕКТИВНОСТІ БЕЗПРОВОДОВОЇ МЕРЕЖІ НА ОСНОВІ НОВІТНЬОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ ARUBA OS 8»**

Виконав: студент 4 курсу, групи КНД–42
спеціальності 122 Комп’ютерні науки
(шифр і назва спеціальності)

Русак Т.І.
(прізвище та ініціали)

Керівник Гніденко М.П
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

Київ – 2021

ВСТУП

На сьогоднішній день існує багато систем, що дозволяють легко розгортати безпроводові мережі на рівні організацій, але Aruba зі своєю операційною системою на фоні своїх конкурентів виділяється певною простотою та зручністю.

Такі слова, як "бездротовий", що описує старовинну радіостанцію, давно забуті в 2021 році. Зараз на ринку існує більше типів бездротового зв'язку, які, як ми думали, будуть можливі ще зовсім недавно, лише 20 років тому, і слово "бездротовий зв'язок" зараз є випадковою назвою для багатьох з них. Однак не всі види бездротового зв'язку однакові, і не всі можуть (або використовуються) в одних і тих самих програмах, наприклад ArubaOS. Деякі з цих термінів можуть бути вам знайомими: радіо- і телевізійне мовлення, радіолокаційний зв’язок, стільниковий зв’язок, глобальні системи позиціонування (GPS), Wi-Fi, Bluetooth та ідентифікація радіочастот - все це приклади «бездротового зв'язку», у деяких випадках із надзвичайно різним використанням .

Важко уявити сучасне життя без всюдисущого WiFi, ця система пройшла довгий шлях з часів свого існування в Австралії в якості експерименту з радіоастрономії в Університеті Маккуорі, і сьогодні близько п'яти мільярдів пристроїв використовують WiFi для роботи в мережі, число яких постійно зростає. WiFi зазвичай використовується для встановлених локальних мереж, де мобільність пристрою є фактором (для ноутбуків та користувачів смартфонів) або де підключення кабелю може бути недоцільним.

WiFi є однією з найбільш трансформаційних технологічних тенденцій останнього десятиліття. Так, існує наявність і зростання очікувань повсюдного зв’язку, незалежно від того, чи це перевірка електронної пошти, проведення голосової розмови, перегляд веб-сторінок чи безліч інших випадків використання. Тепер ми в очікуванні, що зможемо отримати доступ до цих онлайн-сервісів незалежно від місцезнаходження, часу чи обставин: у бігу, стоячи в черзі в офісі, в метро, під час польоту і скрізь між ними.

1 ПОНЯТТЯ БЕЗДРОТОВОЇ МЕРЕЖІ ТА ЇЇ ВИКОРИСТАННЯ

Бездротова мережа відноситься до будь-якого типу комп'ютерної мережі, яка використовує бездротову мережу для мережевих з'єднань. Це метод, за допомогою якого будинки, телекомунікаційні мережі та підприємницькі установи уникають дорогого процесу введення кабелів у будівлю або, як процесс з'єднання, між різними місцями, де розташовується обладнання. Бездротові телекомунікаційні мережі загалом реалізуються та управляються за допомогою радіозв'язку. Це здійснення відбувається на фізичному рівні (Layer) мережевої структури моделі OSI.

Бездротові мережі використовують електромагнітні хвилі для передачі інформації від однієї точки до інший, не покладаючись на будь-який фізичний зв’язок. Радіохвилі часто називають радіо носіями тому що вони просто виконують функцію доставки енергії до віддаленого приймача. Дані, що передаються, накладаються на радіо носій, щоб їх можна було витягти в приймальному кінці. Як тільки дані накладаються на радіо носій, радіосигнал займає більше, ніж єдину частоту, оскільки частота або бітова швидкість модульованої інформації додається до носія. У одному просторі одночасно можуть існувати кілька радіо носіїв, не заважаючи один одному, якщо радіохвилі передаються по інших радіочастотах, для вилучення даних радіоприймач налаштовує одну радіочастоту, відкидаючи всі інші частоти. Потім отриманий модульований сигнал демодулюється і дані витягуються від сигналу.

Насамперед, бездротова мережа - це гнучка система передачі даних, яка використовує такі бездротові носії як радіочастотна технологія для передачі та прийому даних по повітрю, мінімізуючи потребу для дротових з'єднань. Бездротові мережі більш використовуються для доповнення, ніж для заміни дротових мереж і найчастіше їх використовують для забезпечення кількох останніх етапів зв’язку між мобільним користувачем та дротовою мережею.

Наприклад, розглянемо з’єднання Bluetooth та 802.11b, яке в свою чергу може суттєво змінити спосіб використання пристроїв для підключення і комунікацій у повсякденному житті. **Bluetooth** - це малопотужна технологія короткого радіусу дії для спеціальної заміни кабелю; це дозволяє людям бездротово поєднувати пристрої, де завгодно.

І навпаки, **802.11b** - це технологія помірного діапазону і помірної швидкості, розроблена на Ethernet; це дозволяє людям бездротовий доступ до організаційної мережі по всьому місцезнаходженню кампусу. Хоча технології поділяють діапазон 2,4 ГГц та мають деякі програми, що потенційно перекриваються і зіткнувшись один з одним, вони не змагаються і навіть можуть бути успішно поєднані для спільного використання.

Дивлячись на це, зрозуміло що бездротові технології будуть продовжувати свій розвиток, підвищувати рівень нашого життя, роблячи нас мобільними та звищувати змогу контакту один з одним, тим самим прибираючи такий бар’єр, як відстань.

1.1 Переваги та потреби бездротової мережі

До переваг бездротових мереж належать:

1. Бездротові маршрутизатори оснащені модемом, мережевим комутатором (пристроєм, який має кілька порти підключення для підключення комп'ютерів та інших мережевих пристроїв), бездротовий доступ балів.

2. Бездротовий маршрутизатор можна підключити до / з будь-якої точки вашого найближчого оточення або будинку. Це означає, що ви можете входити в Інтернет і користуватися ними в Інтернеті з будь-якого місця навколо вас оточення.

3. Деякі бездротові маршрутизатори оснащені вбудованим брандмауером для захисту від зловмисників. Варіанти конфігурації брандмауера є важливим фактором при покупці маршрутизатора. Практично кожен купує та продає в Інтернеті так чи інакше, купуючи бездротовий маршрутизатор хороші параметри

конфігурації брандмауера можуть бути корисними для безпеки та конфіденційності.

4. Широкосмуговий маршрутизатор бездротової технології VoIP дозволяє підключатися до Інтернету, за допомогою будь-якого звичайного телефонного пристрою. Потім ви можете телефонувати будь-кому в світі через з'єднання з Інтернетом. Бездротовий маршрутизатор забезпечує надійне шифрування (WPA або AES) і оснащений фільтрами MAC-адреси та контролем за автентифікацією SSID.

Бездротові локальні мережі (WLAN) еволюціонували разом з ростом кількості та різноманітності мобільних пристроїв. Кількість пристроїв, що підтримують Wi-Fi, продовжує зростати і зараз. Термін Wi-Fi – це скорочення, означаюче бездротову точність для пристроїв з підтримкою стандарту бездротового зв'язку IEEE 802.11. Це означає, що пристрій сертифіковано на відповідність стандартам сумісності, що були засновані Wi-Fi Alliance. Тип пристроїв, що включають підтримку Wi-Fi, продовжує поширюватися від ноутбуків до багатьох інших пристроїв, таких як камери, телефони, автомобілі та інші споживчі пристрої.

Використання Wi-Fi розширилось за рамки простого використання даних, часто включаючи голосові, відео та інноваційні контекстні програми. Контекстне використання - це поєднання послуги передачі даних, голосу та відео з інформацією, що надається мережею передачі даних, наприклад як розташування пристрою, положення безпеки або доступ до інформації про тип носія. Контекстуальні додатки збільшують цінність або актуальність служби передачі даних, використовуючи додаткові метадані, надані бездротовою мережею. Прикладом контекстної програми даних може бути диспетчерська ремонтна система, що генерує робочі замовлення, використовуючи інформацію про місцезнаходження WLAN для відправлення найближчих техніків для ремонту несправного пристрою.

Очевидно, що WLAN став важливим компонентом для більшості організацій і є критично важливими для багатьох з них. Збільшення залежності

від бездротових локальних мереж збільшило охоплення, безпеку, продуктивність та вимоги до надійності.

1.2 Типи бездротової мережі

Бездротова мережа з'єднує два або більше двох комп'ютерів засобами зв'язку без допомоги проводів. Бездротові мережі використовують спектральний метод або OFDM, в залежності від технології, яка використовується. Бездротова мережа дозволяє користувачеві рухатися в межах широкого покриття і все одно бути пов'язаними з мережею. Існують різні типи бездротових мереж як глобальна мережа, локальна мережа та персональна мережа, але найпоширенішими з них є дві.

1.2.1 Wireless PANs

Бездротові персональні мережі (WPAN) з'єднують пристрої на відносно невеликій території, як правило, в межах досяжності людини. Наприклад, як Bluetooth, так і невидимий ІК порт забезпечує WPAN для підключення гарнітури до ноутбука. ZigBee також підтримує WPAN додатків. PANs мережі Wi-Fi стають звичним явищем (2010 р.), коли розробники обладнання почали інтегрувати Wi-Fi у різноманітні споживчі електронні пристрої.

Персональні мережі PAN в одному важливому відношенні дещо відрізняються від WAN та WLAN. У випадках з цими мережами спочатку налаштовуються мережі, які потім використовують пристрої. В випадку з PAN незалежної мережі не існує. Пристрої, що беруть участь у створенні спеціальної мережі, перебувають у межах досяжності і мережа перестає працювати коли пристрої виходять за межі діапазону. Наприклад, використовування ІЧ порту для обміну даними між ноутбуками дуже схоже в цьому аспекті. Ідея виявлення одне

одного бездротовими пристроями дуже важливий і з’являється у багатьох іпостасях.

Для роботи бездротових PAN не потрібно потужних батарей, що робить їх ідеальними для маленьких пристроїв, таких як аудіогарнітури, стільникові телефони, КПК, ігрові елементи управління, GPS-пристрої, цифрові камери, і ноутбуки. На рисунку нижче (Рис. 1.1) продемонстровано декілька типів таких пристроїв. Наприклад, бездротовий PAN дозволяє бездротово слухати музику на гарнітурах зі свого КПК. Або людина може перенести свою телефонну книгу зі свого ноутбука на мобільний телефон. Як і в цих випадках, бездротові PAN усувають обов'язковість використання дротів, які часто заважають користувачам.

Рис. 1.1 – Типи пристроїв, якими можна користуватись за допомогою PAN

1.2.2 Wireless LANs

Бездротова локальна мережа (WiFi) пропонує можливість безперешкодного доступу до мережевих ресурсів навіть у недосяжності дротової установки. У цьому розділі розглянемо детальніше технічні концепції, які керують Wi-Fi та як Wi-Fi працює з іншими конкуруючими технологіями.

WLAN або бездротова локальна мережа - це термін, позначаючий дану локальну мережу, яка не потребує кабелів для підключення різних пристроїв. Натомість для спілкування використовуються радіохвилі. До таких технологій можна віднести IEEE 802.11 та Bluetooth.

Сьогодні більшість технологій, що використовуються для бездротових локальних мереж, використовують ортогональне мультиплексування з розподілом частоти. Це означає, що використовується декілька частот водночас. Сигнали, близькі один до одного, але які належать до різних каналів, не заважають один одному, оскільки використовують різне кодування схеми. Залежно від використовуваного матеріалу, можна покрити від 30 метрів до 100 метрів в приміщенні, тоді як на вулиці, радіус дії становить близько 100-300 м, якщо немає перешкод.

Як ми вже знаємо, WLAN призначена для забезпечення незалежного від місцезнаходження доступу до мережі між пристроями за допомогою радіохвиль без використання дротів. На корпоративному підприємстві бездротові локальні мережі зазвичай реалізуються як остаточна ланка між існуючою дротової мережею та групою клієнтських комп'ютерів, надаючи цим користувачам бездротовий доступ до повних ресурсів та послуг корпоративної мережі в будівлі чи в кампусі. Широке поширення бездротових локальних мереж залежить від галузевої стандартизації для забезпечення продукту сумісність та надійність між різними виробниками.

Основною мотивацією та перевагою бездротових локальних мереж є збільшення мобільності. Мережа, що відв'язана від звичайних мережевих з'єднань, дає можливість користувачі рухатися майже без обмежень і отримати доступ до локальних мереж майже з будь-якого місця (Рис.1.2).

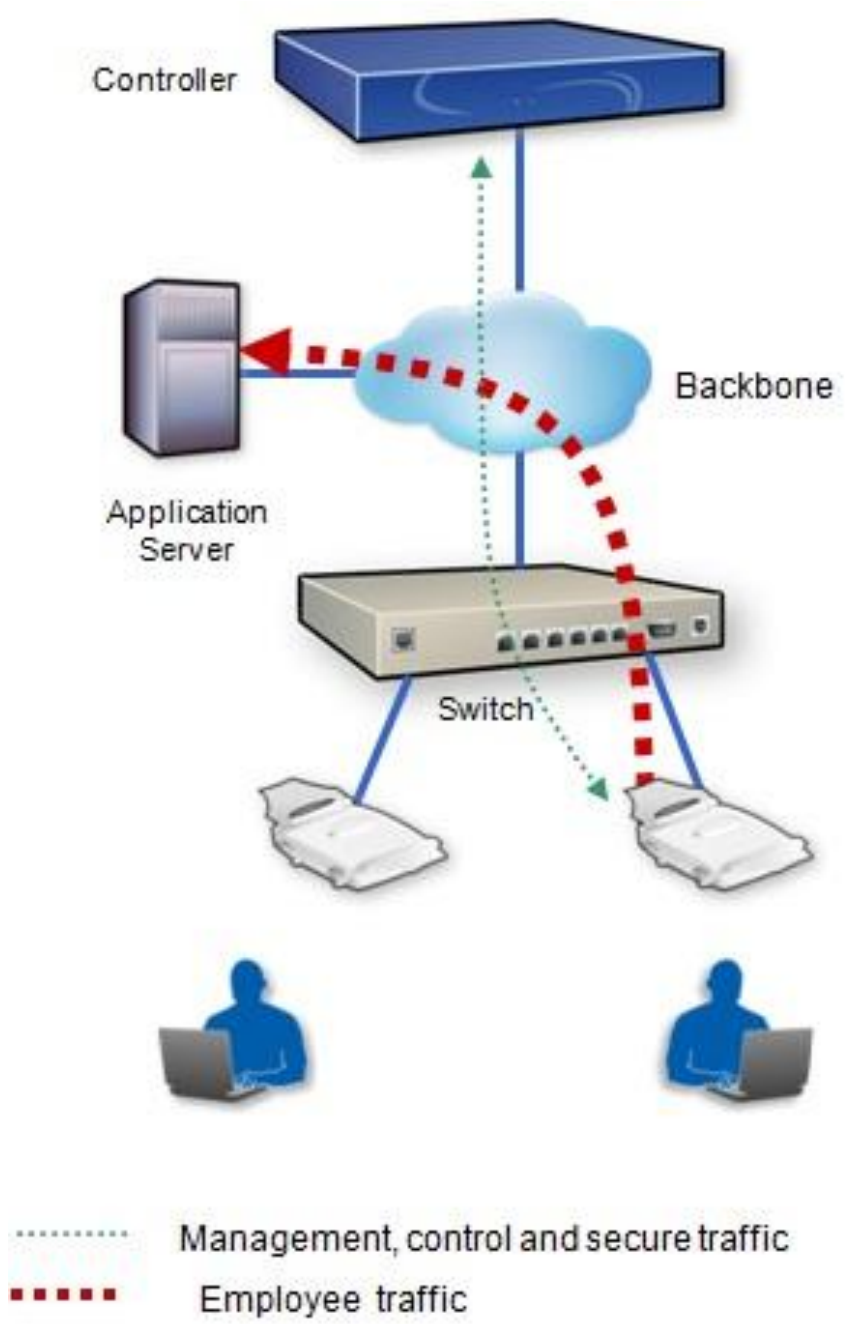

Рис. 1.2 – Модель передачі даних через бездротову мережу

Переваги бездротових локальних мереж:

- Люди можуть отримати доступ до мережі звідки вони хочуть; вони більше не обмежуються довжиною кабелю.
- Деякі міста почали пропонувати бездротові локальні мережі. Це означає, що люди можуть отримати доступ до Інтернет навіть за межами їх звичайного робочого середовища, наприклад, коли вони їдуть додому на тролейбусі.

- Налаштування бездротової локальної мережі можна здійснити за допомогою одної точки доступу. Вона може обробляти різну кількість з'єднань одночасно. Для дротових мереж кабелі мають бути закладеними. Це може бути важко для певних локацій.
- Точки доступу можуть обслуговувати різну кількість комп'ютерів.

Недоліки бездротових локальних мереж:

- Бездротові локальні мережі використовують радіохвилі для зв'язку. Особливу обережність потрібно дотримуватися для шифрування інформація. Також сигнал набагато гірший, і потрібно витратити більше пропускної здатності на виправлення помилок.
- Типова точка доступу IEEE 802.11 має відстань у метрах від місця підключення пристроїв. Щоб розширити діапазон, потрібно більше точок доступу.
- Існує багато проблем із надійністю, особливо пов'язаних з перешкодами від інших пристроїв.
- Бездротові локальні мережі набагато повільніші, ніж дротові; але це може не мати великого значення для більшості користувачів.

1.3 Нові сучасні підходи до організації безпроводових мереж

У двох словах, IoT (Інтернет речей) - це концепція підключення будь-якого пристрою (якщо він має перемикач увімкнення / вимкнення) до Інтернету та інших підключених пристроїв. Internet of Things - це гігантська мережа пов’язаних речей і людей, які збирають та діляться даними про те, як вони використовуються, та про навколишнє середовище. Сюди входить надзвичайна кількість об’єктів будь-якої форми та розміру - від розумних мікрохвильовок, які автоматично готують вашу їжу протягом потрібного періоду часу, до самокерованих автомобілів, чиї складні датчики виявляють предмети на своєму шляху, до

носяться фітнес-приладів, які вимірюють свій пульс і кількість кроків, які ви зробили цього дня, а потім використовуйте цю інформацію, щоб запропонувати спеціальні для вас плани фізичних вправ. Існують навіть підключені футбольні м'ячі, які можуть відстежувати, наскільки далеко і швидко їх кидають, і записувати цю статистику через додаток для майбутніх навчальних цілей. Як це працює? Пристрої та об'єкти з вбудованими датчиками підключені до платформи Internet of Things, яка інтегрує дані з різних пристроїв та застосовує аналітику для обміну найціннішою інформацією із програмами, створеними для задоволення конкретних потреб. Ці потужні платформи IoT можуть точно визначити, яка інформація корисна, а яку можна безпечно ігнорувати. Ця інформація може бути використана для виявлення закономірностей, надання рекомендацій та виявлення можливих проблем до їх виникнення. Наприклад, якщо я є власником автомобілебудівного бізнесу, я міг би знати, які додаткові компоненти (шкіряні сидіння або легкосплавні диски, наприклад) є найбільш популярними. Використовуючи технологію Internet of Things, ми можемо:

- Використовуйте датчики, щоб визначити, які зони у виставковому залі є найпопулярнішими та де клієнти затримуються найдовше;
- Детально ознайомтеся з наявними даними про продаж, щоб визначити, які компоненти продаються найшвидше;
- Автоматично узгоджуйте дані про продажі з пропозицією, щоб популярні товари не зникали.

Інформація, яку отримують підключені пристрої, дозволяє мені приймати розумні рішення щодо того, якими компонентами запастися, на основі інформації в режимі реального часу, що допомагає заощадити час і гроші. Завдяки вдосконаленій аналітиці з’являється можливість зробити процеси ефективнішими. Розумні об'єкти та системи означають, що ви можете автоматизувати певні завдання, особливо коли вони повторюються, буденні, трудомісткі або навіть небезпечні. Як приклад можна привести ситуацію:

Ви прокидаєтесь о 7 ранку щодня, щоб піти на роботу. Ваш будильник чудово справляється з тим, щоб вас розбудити, до тих пір, поки щось не піде не так. Ваш поїзд скасовано, і вам доведеться їхати на роботу. Єдина проблема полягає в тому, що їхати потрібно довше, і вам потрібно було б встати на 15 хвилин раніше, щоб не запізнитися. Також, погода зненацька може зіпсуватися, наприклад може початися дощ і їхати доведеться повільніше, ніж зазвичай. Підключений або ввімкнений IoT будильник перезавантажиться, виходячи з усіх цих факторів, щоб забезпечити вам роботу вчасно. Він може визнати, що ваш звичайний поїзд скасований, розрахувати відстань проїзду та час у дорозі для роботи вашого альтернативного маршруту, перевірити погоду та коефіцієнт зниження швидкості руху через сильний дощ та підрахувати, коли він повинен вас розбудити, щоб ви ' не пізно. Якщо він надзвичайно розумний, може навіть синхронізуватися з вашою кавоваркою з підтримкою IoT, щоб забезпечити готовність вашого ранкового кофеїну, коли ви прокинетесь.

IoT часто привертає увагу споживачів, чий досвід роботи з такими технологіями, як розумні годинники або ж будильники, пом'якшується власними проблемами конфіденційності та безпеки, що пов'язані з постійним зв'язком. Ця споживча точка зору переважна у всіх видах корпоративних проектів IoT, особливо коли кінцевим користувачем є широка громадськість. Рішення корпоративних IoT дозволяють компаніям вдосконалювати існуючі бізнес-моделі та налагоджувати нові зв’язки із клієнтами та партнерами, але не без проблем. Обсяг даних, що видаються системою інтелектуальних пристроїв, може стати надзвичайним (часто описується як великі дані). Інтеграція великих даних у існуючі системи та налаштування аналітики даних на їх дії можуть ускладнитися. Безпека IoT є головним фактором, що створює системи IoT. Тим не менш, для багатьох компаній IoT вартує зусиль, і успішні випадки використання IoT на підприємстві можна знайти майже у кожній галузі.

Існує ще один надійний спосіб – Edge Computing (Граничні обчислення) Це обчислення, які відбуваються у фізичному розташуванні користувача або джерела даних або поблизу нього, що призводить до меншої затримки та економить

пропускну здатність. Розміщуючи обчислювальні послуги ближче до цих місць, користувачі отримують вигоду від швидших, надійніших служб з кращим досвідом роботи, тоді як компанії виграють завдяки кращій підтримці програм, чутливих до затримок, та використовуючи такі технології, як аналіз AI / ML, для виявлення тенденцій та пропонування кращих продуктів. та послуги. Граничні обчислення - це один із способів, яким компанія може використовувати та розподіляти загальний пул ресурсів у великій кількості місць, щоб допомогти масштабувати централізовану інфраструктуру для задоволення потреб зростаючої кількості пристроїв та даних. Шлюз IoT може надсилати дані від краю назад до хмари або централізованого центру обробки даних, або до граничних систем, що обробляються. Локальні обчислення приносять більше обчислювальної потужності до країв мережі з підтримкою IoT, щоб зменшити затримку зв'язку між пристроями з підтримкою IoT та центральними IT-мережами, до яких ці пристрої підключені. Здатність пристроїв обчислювати стає все більш цінною як засіб для швидкого аналізу даних у реальному часі. Просто надсилання або отримання даних означало появу IoT. Але надсилання, отримання та аналіз даних разом із програмами IoT - це майбутнє.

У моделі хмарних обчислень обчислювальні ресурси та послуги часто централізовані у великих центрах обробки даних. Доступ до цих центрів обробки даних здійснюють пристрої з підтримкою IoT на краю мережі. Це модель, яка зменшує деякі витрати та ефективніше розподіляє ресурси. Але ефективний IoT вимагає більшої обчислювальної потужності ближче до місця, де насправді існує фізичний пристрій. Граничні обчислення розподіляють обчислювальні ресурси до цього краю, тоді як всі інші ресурси централізовані в хмарі. Це конкретне розміщення обчислень забезпечує швидку практичну статистику, використовуючи дані, чутливі до часу. Координація парку автомобілів без водіїв, що перевозять контейнери, за допомогою інтелектуальних пристроїв відстеження - це яскравий приклад, але є і багато інших практичних реалізацій.

Розглянемо RFID та транспортну галузь: зв’язок між RFID та зчитувачем завжди є одним із способів. RFID не може отримувати оновлення так само, як

центральна IT-мережа не може передавати дані назад до RFID. Це не система постійного моніторингу, що означає, що відстеження логістики обмежується реєстрацією в певних місцях. Але якщо пристрій IoT може координувати роботу з датчиками IoT, встановленими в транспортних засобах, які їх перевозять, усіма даними може управляти центральна IT-мережа. Але цей підключений сценарій означає, що кожному фізичному пристрою IoT потрібно багато обчислювальної потужності, особливо якщо ця логістична компанія використовує складні машини, такі як автомобілі без драйверів. Замість простого надсилання та отримання - завжди чекаючи інструкцій від централізованого центру обробки даних через Wi-Fi, пристроям IoT потрібно буде обробляти дані самостійно та приймати обґрунтовані рішення. Ця реалізація обчислювальної потужності ближче до зовнішніх країв мережі, а не до централізованого центру обробки даних, відома як обчислення краю. В якості останнього прикладу розглянемо будівельний майданчик. Можливо, будівельна компанія привезла на роботу машину з підтримкою Bluetooth. Ця машина передає дані через смартфони працівників, що допомагає компанії відстежувати використання машини та її розташування. Якщо 10 співробітників працюють навколо цього пристрою протягом усього дня, їх смартфони постійно перевіряють сервер cental - описуючи місце розташування машини. Ця надмірна діяльність сервера може перевантажити IT-систему. Але мобільний додаток IoT може використовувати смартфон як невеликий, малопотужний сервер і зменшити зайві пінги до центрального сервера.

Таким чином, зрозуміло, що безпроводові мережі розвиваються з великою швидкістю, та мають великий попит у сьогоденному розвитку організацій. Існує велика кількість можливостей та способів, але найкращим являється розгортання локальних мереж WLAN. У цієї мережі є багато переваг, але існують і недоліки, котрі являються не дуже значними у виборі WLAN, що робить її найкращим рішенням для організацій і не тільки.

2 ДОСЛІДЖЕННЯ ТА ОПИС ПРОДУКТУ ARUBA OS 8

ArubaOS - це мережева операційна система (NOS), розроблена компанією Aruba, яка є дочірньою компанією Hewlett Packard. Як і більшість платформ мережевих ОС, ArubaOS забезпечує управління та підтримку мережевих комп'ютерів.

Більшість систем допомагають мережевим комп’ютерам якомога ефективніше використовувати спільні ресурси, що робить їх чудовими для локальних мереж та глобальних мереж, в особливості для зростаючого ринку SD-WAN для корпоративних підприємств.

Багато мережевих операційних систем існують насамперед для підтримки підключення апаратних ресурсів, таких як сервери, принтери та навіть можливості багатопроцесорної обробки. Задля того, щоб інкапсулювати деякі найсучасніші функціональні можливості мережі, якими сьогодні користуються підприємства, ArubaOS розширює функції NOS, а саме такі як:

- Безпека мережі;
- Голосові та відео послуги;
- Хмарні сервіси;
- Пристрої Інтернету речей (IoT).

Дивлячись на такий функціонал, неможливо не побачити зосередження ArubaOS на продуктивності, безпеці та надійності, що робить його чудовим продуктом для корпоративних підприємств, котрі працюють в критично важливих мережевих технологіях.

2.1 Архітектура

Більшість пристроїв кінцевих користувачів у сучасних виробничих мережах це бездротові пристрої, включаючи ноутбуки, котрі постачаються без порту Ethernet. Дротові телефони замінюються на уніфікований зв’язок, використовують такі програми, як Skype for Business (Skype для бізнесу), і ці тенденції змушують підприємства все більше покладатися на бездротові локальні мережі (LAN) для задоволення їхніх бізнес-потреб. З найважливішими залежностями від LAN, адміністратори мережі повинні розробляти складні мережі для підтримки різних типів додатків, користувачів та пристроїв без шкоди для безпеки.

Завдяки широкому набору інтегрованих технологій та можливостей, ArubaOS 8 забезпечує уніфікований дротовий та бездротовий доступ, безшовний роумінг, корпоративну безпеку та високодоступну мережу з необхідною продуктивністю, досвідом роботи та надійністю для підтримки середовищ з високою щільністю.

Таблиця 2.1 – Портфоліо контролера

Controller Series	**Controller Model**	**Number of APs**	**Number of Users**	**Firewall (Gbps)**
70xx	7005	16	1,024	2
	7008	16	1,024	2
	7010	32	2,048	4
	7024	32	2,048	4
	7030	64	4,096	8
72xx	7205	256	8000	12
	7210	512	16000	20
	7220	1,024	24000	40
	7240	2,048	32000	40
	7280	2,048	32000	100
ArubaOS 8.x не підтримує контролери серії 3000 або 600.				

Існують спеціальні режими контролера, які підтримує ArubaOS 8. Ці режими дозволяють гнучко регулювати параметри обміну між контролерами через Інтернет. Вони можуть бути підключені до Інтернету двома способами:

1. Через широкосмуговий доступ до Інтернету (за технологією ethernet);
2. Через бездротовий доступ до Інтернету (GPRS, 3G).

Один з таких режимів називається **Mobility Master** (укр. Майстер Мобільності), його концепція зовсім нова для ArubaOS 8. Mobility Master можна класифікувати, як Virtual Mobility Master (VMM) та як Hardware Mobility Master (HMM). Mobility Master призначений для роботи на платформах з розрядністю x86, а функції представлені в ArubaOS 8, потребують центральну оперативну пам'ять (RAM), процесор (CPU) та простір для зберігання, що не підтримується фізичними контролерами.

Mobility Master має бути повністю налаштований адміністратором мережі, подібно до того, як головний контролер має бути налаштований в ArubaOS 6. Основна роль Mobility Master (Рис. 2.1) полягає в тому, щоб служити єдиною точкою конфігурації та управління зображеннями для мережі.

Крім того, Mobility Master можна налаштувати за допомогою Північного інтерфейсу прикладних програм (NBAPI - Northbound Application Programmable Interface). Virtual Mobility Master можна встановити на VMWare, KVM або Hyper-V в залежності від того, що найбільш підходить для розгортання. HMM та VMM альтернативно можуть позначатися як MM-HW та MM-VA, що означає апаратне забезпечення MM-Hardware та віртуальний пристрій MM-Virtual Appliance, відповідно. До речі, точки доступу, які призначені для забезпечення бездротового доступу до мережі що існує, не можуть бути припинені на MM.

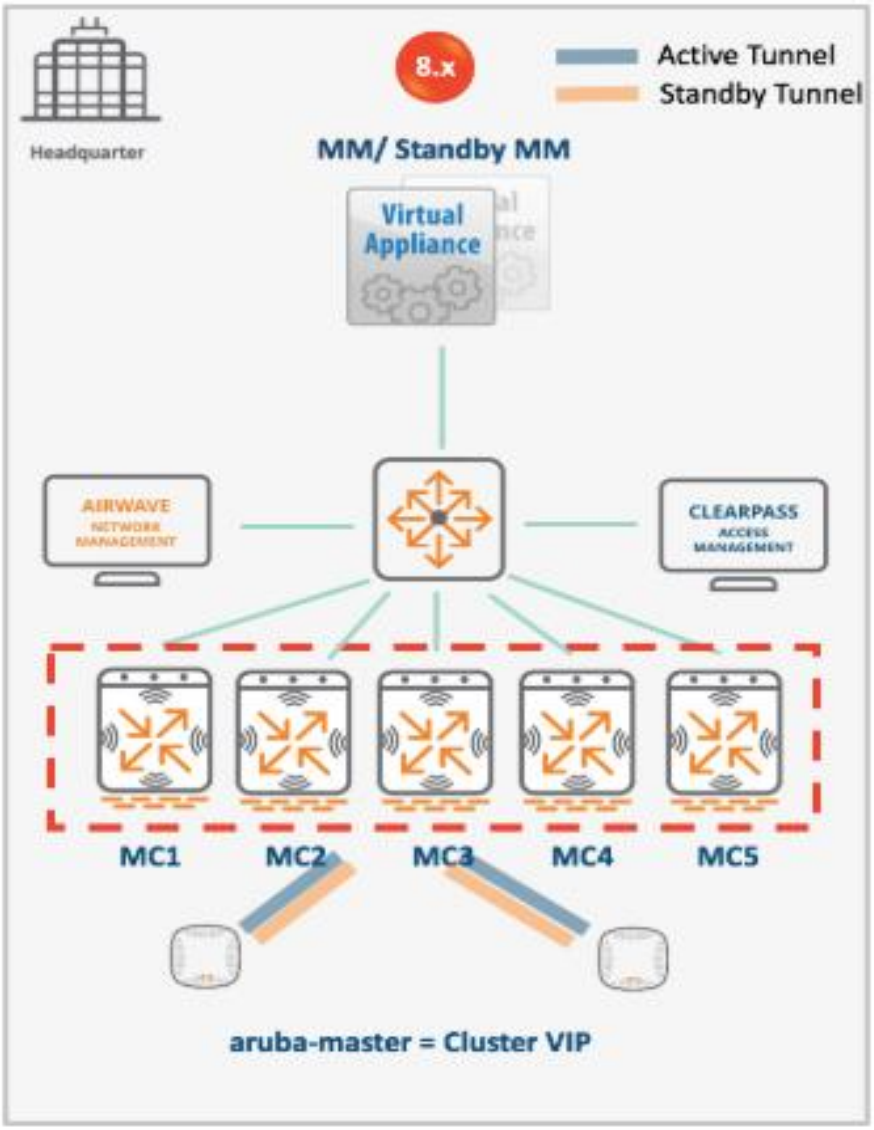

Рис. 2.1. Модель Mobility Master

ArubaOS 8 також демонструє користувачам концепцію режиму головного контролера (MCM – Master Controller Mode), задля забезпечення плавного переходу від ArubaOS 6, не вимагаючи пристрою на базі x86 (HMM) або VMM. MCM також може керувати іншими контролерами (MC), але однак доступна лише підмножина функцій MM, тим самим точки доступу не можуть бути припинені, оскільки вони будуть налаштовані за допомогою Mobility Master. Тільки контролери 7030 та серії 72xx контролери підтримують режим головного контролера.

Таблиця 2.2 – Матриця функцій Master Controller Mode

Підтримувані функції	**Непідтримувані функції**
Новий веб-інтерфейс, робочі цикли та ієрархічна конфігурація	Кластеризація
Мультизона	AirMatch
Багатопотоковий CLI з автовиконанням	Централізована підтримка додатків (UCC, AppRF)
Зв'язок WAN та балансування завантаження	Оновлення у реальному часі
Розподілені UCC, AppRF, ARM та AirGroup	Централізована видимість

Концепція контролера мобільності (MC - Mobility Controller) також є новою для ArubaOS 8. MC схожий на контролер відділення в ArubaOS 6, так як це може бути налаштовано за допомогою ZTP та Aruba Activate. Останній порт контролера мобільності ввімкнено як DHCP-клієнт на VLAN 4094 у заводській конфігурації за замовчуванням. MM та MCM не можуть прийняти MC, використовуючи DHCP Option 43, оскільки сертифікат розподілу MM або MCM не підтримується параметрами DHCP.

На відміну від локальних контролерів ArubaOS 6, контролерами мобільності можна повністю керувати MM (Рис. 2.2) або MCM. Крім того, адміністратор може налаштувати всі функції контролера мобільності. Контролери серії 70xx та 72xx поставляються як контролери мобільності. ArubaOS 8 також підтримує Віртуальні контролери мобільності (VMC - Virtual Mobility Controllers). VMC можна поставити на VMWare, KVM або Hyper-V. Контролери мобільності також можна налаштувати як концентратори віртуальних приватних мереж (VPNC - Virtual Private Network Concentrators).

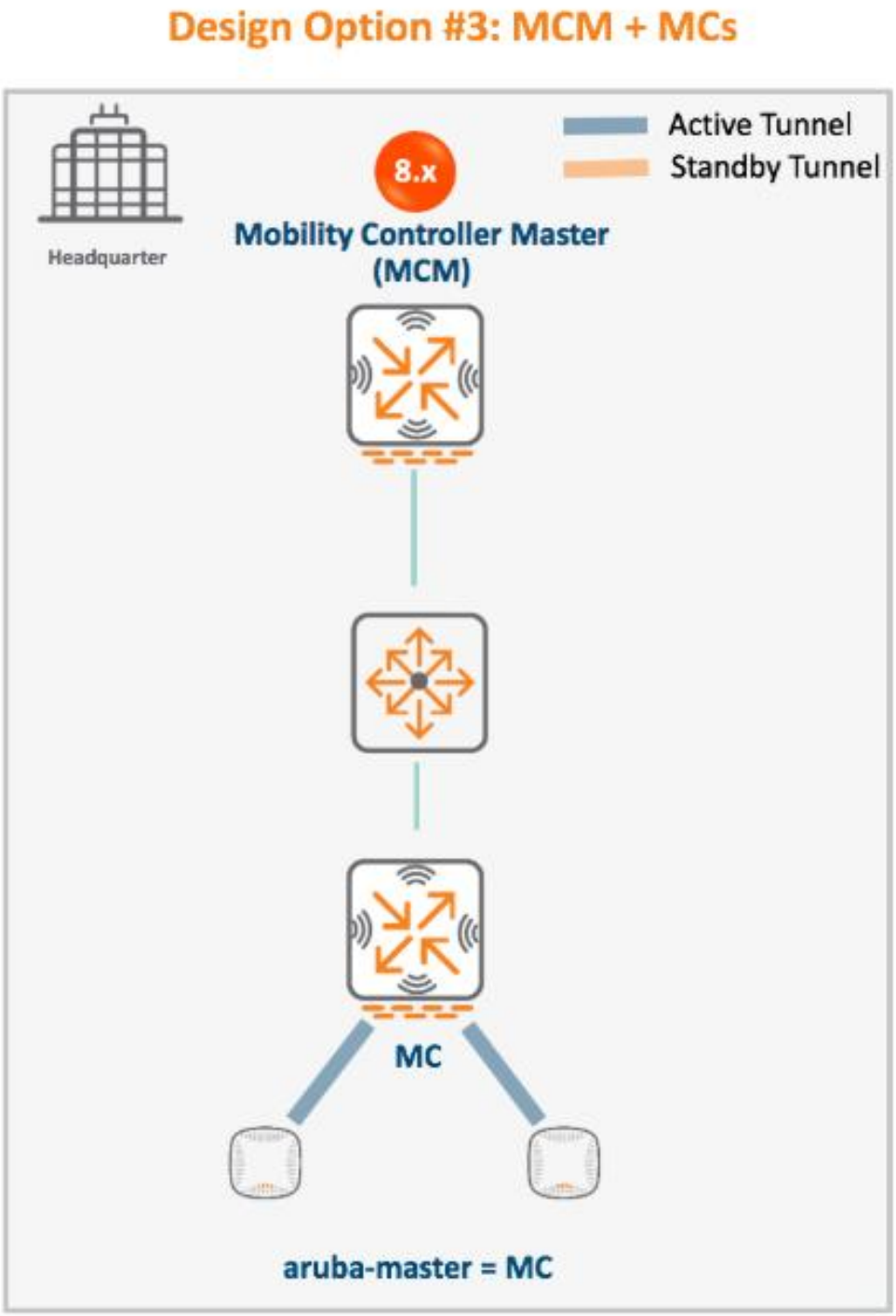

Рис. 2.2 - Модель Mobility Controller Master

ArubaOS 8 також може налаштувати автономний контролер (Stand-alone Controller) (Рис. 2.3). Автономний контролер не може керуватись ММ і не може бути в одній групі з іншими автономними контролерами. Він дуже схожий на Stand-alone контролери в ArubaOS 6 і підтримує функцію Multizone. AirMatch та кластеризація не ввімкнені на окремих контролерах, оскільки їх можна лише реалізувати за допомогою віртуальної машини (VM - Virtual Machine). **ARM** -

єдиний доступний метод оптимізації радіочастот. Інші функції такі, як WebCC, AppRF, UCC, AirGroup, Northbound API, UCM та WMS будуть функціонувати як і раніше на локальному контролері ArubaOS 6.

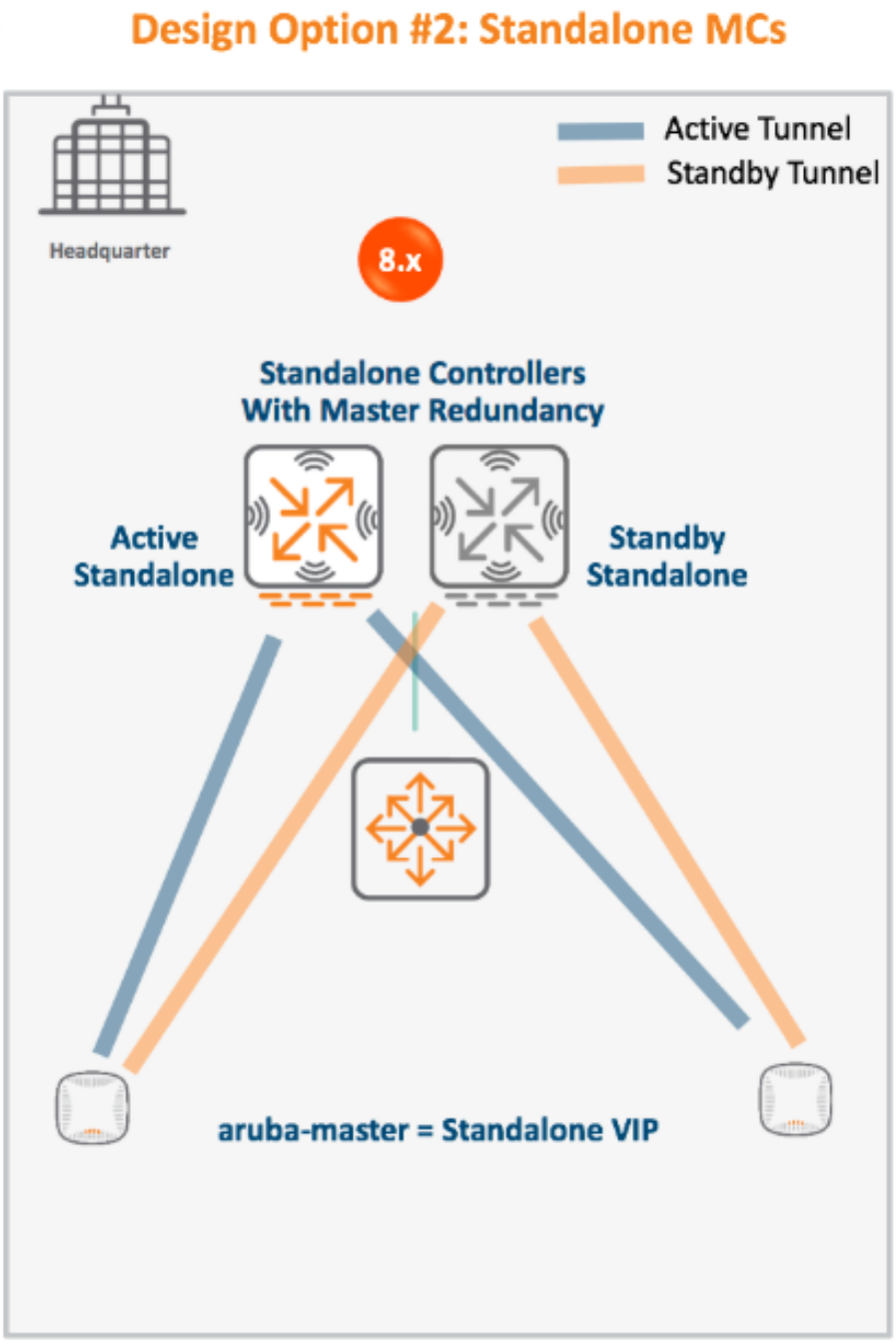

Рис. 2.3 - Модель автономного Stand-alone контролера

Міграція з топології ArubaOS 6 на топологію ArubaOS 8 в основному складається із заміни Master Controller на Mobility Master та заміни усіх локальних та гілкових контролерів на Mobility Controller.

Водночас архітектура AOS 8 представила **Mobility Conductor (MCR)** як центральну точку конфігурації та моніторингу. Трохи нижче (рис.6) можна побачити приклад типової топології корпоративної мережі, яка показує MCR, що вона керує кількома керованими пристроями (**MD – Managed Devices**), які припиняють роботу з точками доступу. Конфігурація для всіх MD та точок доступу виконується за допомогою MCR, спрощуючи конфігурацію, не вимагаючи управління кожним MD окремо.

До появи ArubaOS 8.0.0.0 єдиним способом налаштування MCR / MD було використання інтерфейсу командного рядка **(CLI – Command Line Interface)** або вебінтерфейсу користувача **(WebUI – Web User Interface)**. Разом з AOS 8 був введений інтерфейс програмування програм **(API – Application Programming Interface)**, тим самим створивши необхідну можливість для автоматизації на основі API для бездротової локальної мережі на базі Aruba AOS 8, не зважаючи на це CLI все ще залишається популярним інтерфейсом для автоматизації мережі через наявні середовища. API AOS 8 доступний на кондукторі мобільності (Mobility Conductor), який є централізованою точкою конфігурації. Автоматизація мережі на основі API або CLI може бути виконана на кондукторі мобільності для ефективного управління конфігурацією пристроями.

ArubaOS 8 представила новий спосіб управління конфігурацією через мобільні провідники та керовані пристрої, використовуючи концепцію ієрархічного управління. Однак, зазначу, що також важливо розуміти цю конструкцію конфігурації, щоб спростити та автоматизувати управління конфігурацією (Рис 2.4).

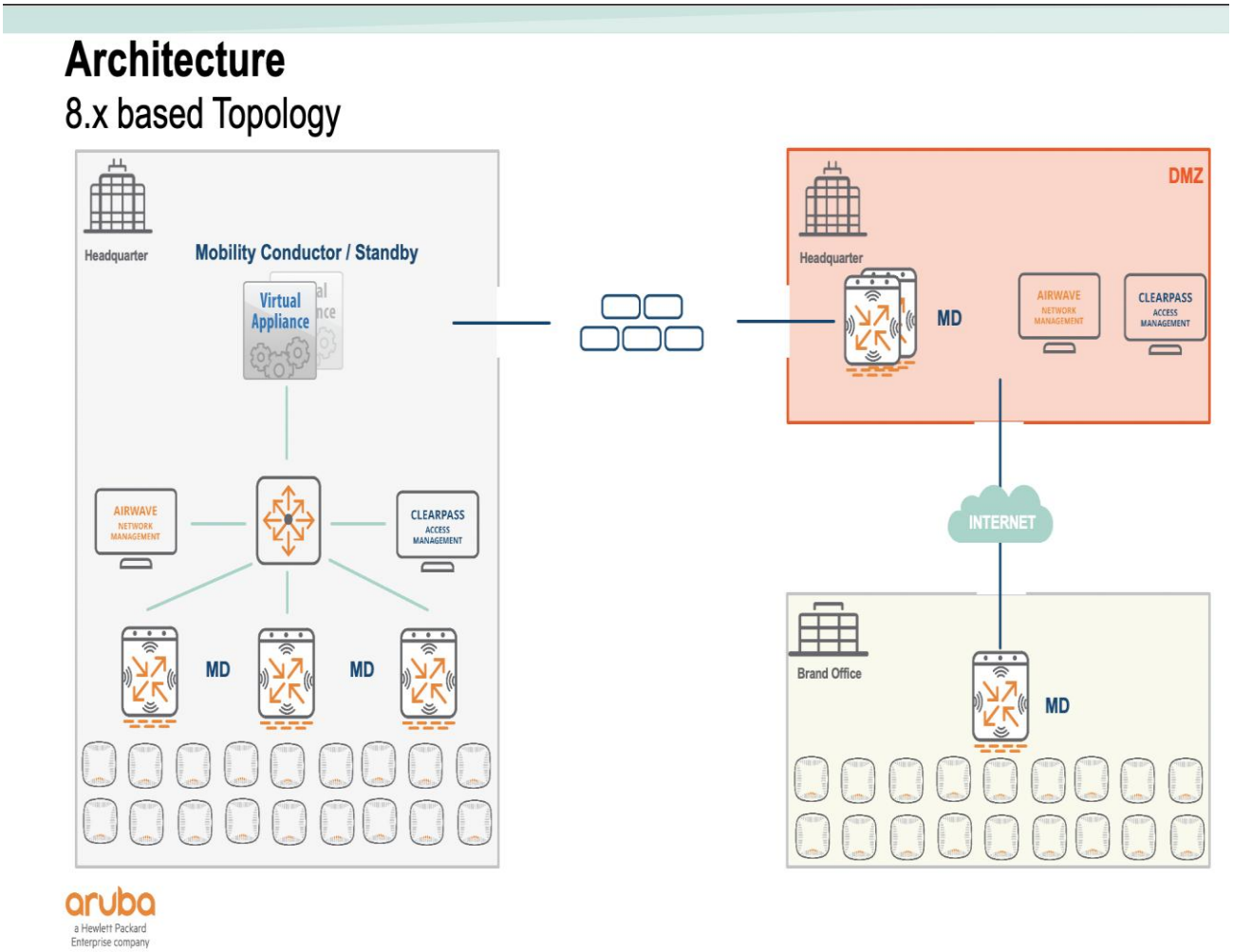

Рис. 2.4 - Топологія ArubaOS 8

Відмінності топології ArubaOS 6 від топології ArubaOS 8:

1. Представлення Mobility Master на основі віртуальної машини (VM), як єдиної точки конфігурації та управління зображеннями;
2. Представлені контролери мобільності, якими повністю керує Mobility Master за допомогою ZTP.
3. Mobility Master не припиняє роботу з точками доступу.
4. Контролери 72xx та 70xx можуть бути встановлені, як контролери мобільності або автономні stand-alone контролери.
5. Введено режим головного контролера MCM, як шлях міграції.

Таблиця 2.3 – Змінені позначення пристроїв контролерів на базі ArubaOS 6 та їх аналоги на базі ArubaOS 8

ArubaOs 6	**ArubaOS 8**
Головний контролер (Master Controller)	Mobility Master (VM або апаратне забезпечення) або Master Режим контролера (лише 72xx та контролери 7030)
Локальний контролер (Local Controller)	Контролери мобільності (Mobility Controllers)
Контролер відділення (Branch Controller)	Контролери мобільності (Mobility Controllers)
Автономний контролер (Stand-alone Controller)	Автономний контролер (Stand-alone Controller)

2.2 Ієрархія та удосконалення конфігурації AOS

Ієрархічна конфігурація представлена в ArubaOS 8 (Рис. 2.5) задля покращення способу застосування конфігурацій розгортання декількох контролерів. AOS 8 представляє концепцію ієрархічної конфігурації та ZTP для всіх режимів розгортання. Новий контролер кампусу або контролер відділення може виявити те, що Mobility Master використовує параметри DHCP або Aruba Activate та отримати всю їхню конфігурацію від Mobility Master. Незважаючи на масштаб контролерів, котрі керуються, Mobility Master діє як єдина точка дотику для всього розгортання.

Під вузлом керованої мережі можна створити максимум чотири вкладені дочірні вузли. Для спрощення управління конфігурацією рекомендується створювати стільки вкладених вузлів, скільки насправді потребується.

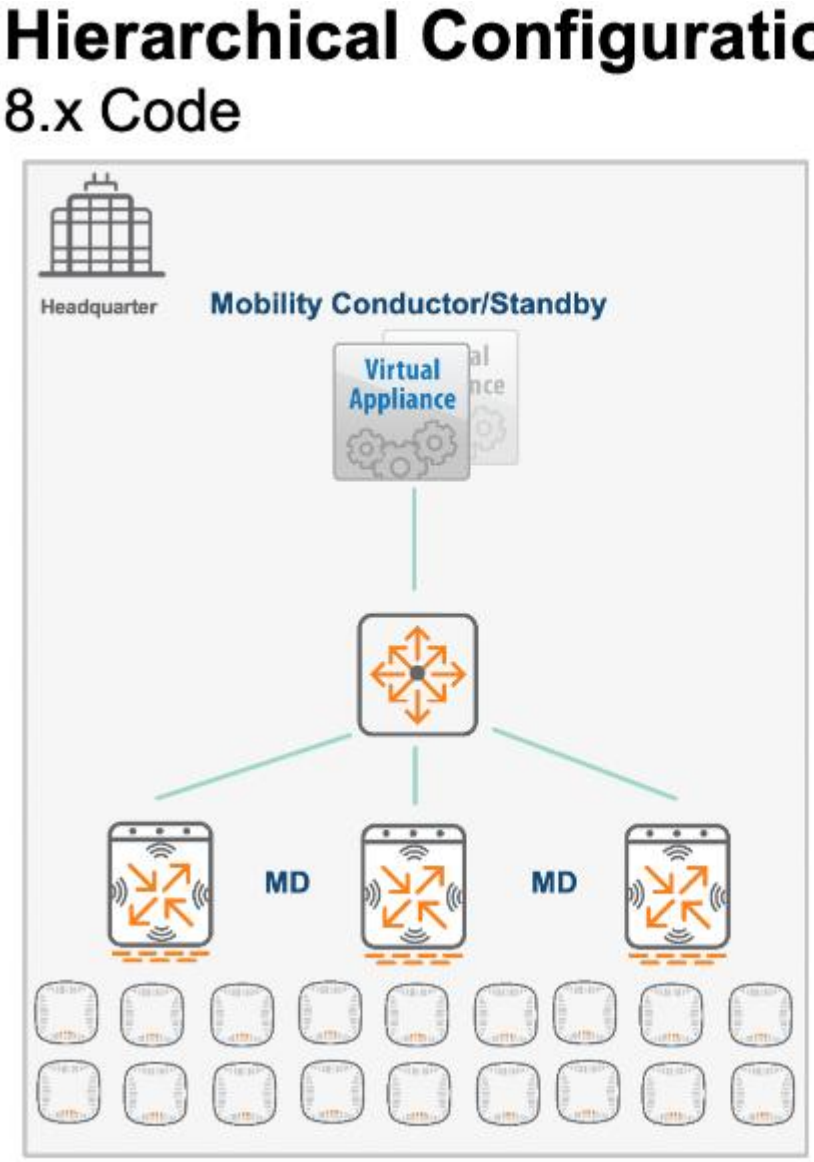

Рис. 2.5 - Звичайна конфігурація ArubaOS 8

Дана ієрархічна конфігурація дає змогу створювати вузли конфігурації на Mobility Master, який має загальні конфігурації для певного регіону, кампусу чи будівлі. Як тільки контролер буде внесений до білого списку вузла конфігурації, тоді конфігурації на рівні пристрою можна додати до вузла конфігурації пристрою. Коли контролер мобільності вперше контактує з Mobility Master, конфігурація рівня групи об’єднана з конфігурацією рівня пристрою, а потім надсилається до контролера мобільності.

Aruba нерідко рекомендує визначати конфігурації на вузлі під вузлом Managed Network, а не на самому вузлі керованої мережі. Це робиться для

забезпечення достатнього зростання мережі та масштабованість, одночасно підтримуючи окрему ієрархію конфігурації для нових сайтів. При конфігурації на керованій мережі вузол повинен бути мінімальним, щоб запобігти поширенню проблем, пов’язаних з неправильною конфігурацією на кожному другому вузлі в ієрархії.

2.2.1 Системні вузли

В той час, як система працює з декількома вузлами, їм присвоюються різні ролі, мітки та їх стан може змінюватися. Mobility Master використовує додаток для централізованої конфігурації, щоб підтримувати всі конфігурації в домені управління, виключаючи використання декількох точок контакту для застосування глобальних та локальних конфігурацій до кожного керованого пристрою, тим самим це дозволяє нам організувати всі типові конфігурації на вищому рівні ієрархії.

За замовчуванням вузли системного рівня присутні у **WebUI** мобільного мастера і їх неможливо видалити. Системні вузли наведені нижче:

- **MM** - у випадку надлишкових майстрів мобільності конфігурація, визначена на цьому вузлі (Рис. 2.6), є спільною для обох активних та в режимі очікування майстрів мобільності.
- **Ім'я хосту** (Hostname of MM)- містить в собі конфігурацію для фактичного Mobility Master.
- **Керована мережа** (Managed Network) - ієрархія, за якої створюються всі визначені користувачем вузли та налаштовано контролери.

2.2.2 Користувацькі вузли

Користувацькі вузли створюються адміністраторами під системним вузлом Managed Network. Ієрархія вузлів може бути створена під цим вузлом, де всі

верхні вузли мають загальну для всіх контролерів конфігурацію. В той час, вона стає більш конкретною (в залежності від регіону, кампусу чи будівлі) на нижчих рівнях ієрархії. За звичай вузли пристрою (Рис. 2.7) визначені у самому низу.

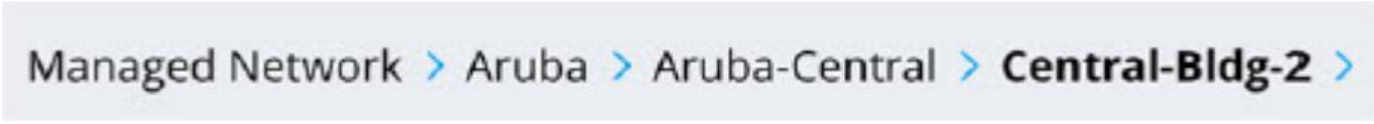

Рис. 2.6 - Груповий вузол

Рис. 2.7 - Вузол пристрою

Таблиця 2.4 – Вузли та їх структура

Категорія	Ім`я вузла	Опис вузла
Mobility Master	/	Конфігурації, загальні для Mobility Master та керованих ним пристроїв (кореневий вузол). **Нотаток**: Зміни конфігурації заборонені корневим вузлом.
	/md	Конфігурації, загальні для всіх керованих пристроїв. Користувач має змогу створити додатковий вузол під цим вузлом.
	/mm	Конфігурації, загальні для основного та резервного Mobility Master (пара VRRP).
	/mm/mynode	Конфігурації специфічні до конкретного Mobility Master. Зміни можуть бути лише відповідно Mobility Master.
Stand-alone Controller	/mm	Конфігурації, загальні для основного та резервного автономного контролерів (пара VRRP).
	/mm/mynode	Конфігурації специфічні до конкретного автономного контролера. Зміни можуть бути лише відповідно автономного контролера.
Managed Device	/mm	Конфігурації синхронізовано з Mobility Master.
	/mm/mynode	Конфігурації виконано локально на керованому пристрої (віддалене скасування). **Нотаток:** Ці вузли не можуть бути переглянутими або доступними на Mobility Master.
Термін «mm» посилається до Mobility Master, та «md» - до керуючого пристрою.		

2.2.3 Адміністрування рівня вузла та дизайн ієрархії вузла

Ієрархічна конфігурація дозволяє створювати облікові записи адміністрування на рівні вузла на Mobility Master. Мережеві адміністратори можуть повністю керувати конфігурацією для контролерів, встановлених у вузлі та нижче конфігурації вузлів, для яких вони мають необхідні дозволи для доступу до рівня регіону, кампусу чи будівлі без жодного впливу на контролери в інших місцях ієрархії (Рис. 2.8). Ця функція гарантує, що будь-які небажані зміни конфігурації, внесені на локальних сайтах, не будуть впливати на всю організацію.

Тестування доказовості концепції - це ще один варіант використання, коли власні збірки та функції ArubaOS повинні бути перевірені у лабораторії перед тим, як вводити їх у виробництво. У такому випадку можна створити тестові вузли конфігурації разом із адміністративними обліковими записами на рівні вузла. Оскільки вузли створюються в середовищі пісочниці, тестування може бути виконано вільно та без небажаних ефектів вище в конфігурації ієрархії.

Щодо дизайну ієрархії вузлів, ієрархічні конфігурації повинні бути розроблені таким чином, щоб конфігурації, які є загальними для організації, перебували на вузлах вищого рівня. Решту конфігурації успадкує нижчі
вузли ієрархії, так як вимоги до мережі стають більш конкретними. Наприклад, названий VLAN може бути визначеним на вищому рівні ієрархії, а потім присвоюється з певними VLAN ID на нижчих рівнях. Нарешті, конфігурації, характерні для окремих контролерів, такі як фізичний і віртуальний інтерфейси, IP-адреси, та членство в кластері налаштовується на вузлах рівня пристрою. Усі конфігурації, які залежать від одного вузла завжди потрібно визначати разом у загальному вузлі, наприклад, визначаючи VLAN ID та VLAN.

Нижче наведено підходи до реалізації ієрархічного проектування:

- Ієрархія конфігурації зазвичай створюється на основі географічної сегментації контролерів. Якщо організація має кілька офісів по всій країні, то для кожного слід створити вузли конфігурації для кожного регіону, такі як Східний, Центральний та Західний. Кожен із цих регіонів, у свою чергу, може мати кілька кампусів, будівель та пристроїв, котрі матимуть власний вузол конфігурації.
- Альтернативний спосіб організації ієрархії може базуватися на типі пропонованих послуг, таких як кампус та дистанційний з регіональними варіаціями внизу родоводу.

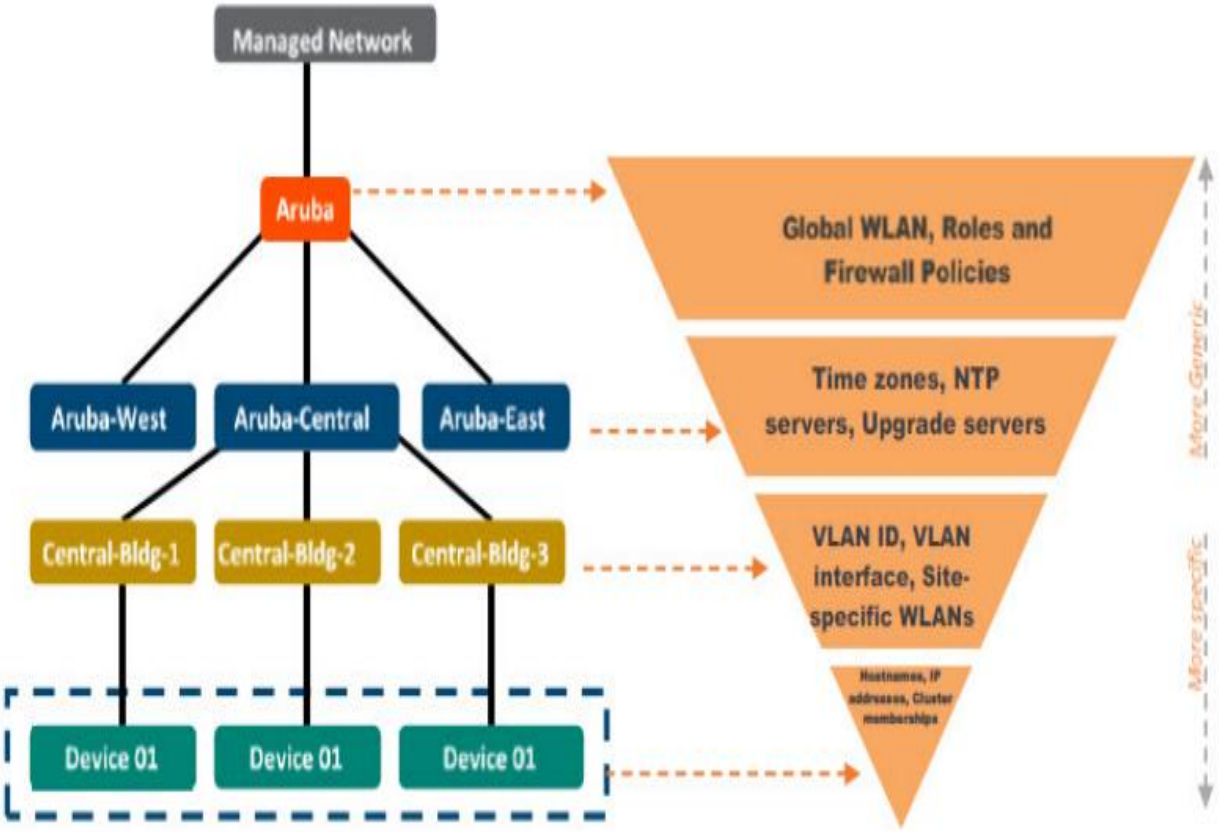

Рис. 2.8. Дизайн ієрархії вузла

2.3 Ліцензування

ArubaOS підтримує централізоване ліцензування ще з ArubaOS 6. Ліцензії встановлюються на одному контролері, а інші контролери підписуються на вилучення ліцензій із глобального пулу ліцензій, якщо потрібно. Однак суттєвим обмеженням для цієї моделі було те, що в деяких розгортаннях клієнтів не було можливості контролювати кількість ліцензій,котрі один контролер міг вилучити з пулу. Це обмеження призвело до таких ситуацій, коли, наприклад, пули ліцензій вичерпаються і на одному сайті буде розгорнуто більше точок доступу, ніж було наявних ліцензій у пулі.

З появою ArubaOS 8, Mobility Master тепер підтримує створення менших ліцензованих пулів в рамках глобального пулу. Цей метод сегментації дозволяє обмежувати або резервувати ліцензії, які певний контролер або група контролерів можуть вилучити з глобального пулу.

Більшість ключових можливостей та функцій платформи ArubaOS 8 увімкнено за допомогою ліцензій. Ці ліцензії зазвичай встановлюються на Mobility Master, але також можуть бути встановлені на MCM або автономних контролерах, якщо це потрібно. Крім того, централізоване ліцензування, під управлінням Mobility Master або MCM, дозволяє контролерам мобільності записувати необхідну кількість ліцензій.

З новим Mobility Master з’являється ще одна ліцензія. Ліцензія називається "MM-VA-XX" або "MM-HW-XX", залежно від того, купуєте ви віртуальний пристрій або апаратний пристрій. Ця ліцензія дає вам право керувати кожним контролером мобільності та точкою доступу у вашому середовищі. Якщо ваш Mobility Master - це віртуальний пристрій, це ліцензія на кожен пристрій, яка продається блоками з ліцензіями 50, 500, 1K, 5K та 10K. Якщо ви виберете апаратний пристрій, то ліцензії MM вбудовані в прилад, що підтримує пристрої 1K, 5K або 10K. У більшості випадків розгортається віртуальний Mobility Master. Це дозволяє середовищу бути більш гнучким і використовувати надмірність,

вбудовану у віртуальне середовище. Другу головну віртуальну машину мобільності можна створити для надмірності без будь-яких додаткових витрат.

Mobility Master в ArubaOS 8 служить централізованим сервером ліцензування для контролерів мобільності під його управлінням. Точки доступу та контролери отримуватимуть з централізованого пулу ліцензій Mobility Master, коли він виконує функції ліцензування. Споживання ліцензії VMM відбувається за допомогою дещо іншого методу, оскільки ці машини є віртуальними. Потрібно придбати лише одну ліцензію MM-VA-XX, навіть якщо кілька VMM розгорнуто для резервування. Якщо VMM використовується для підтримки до 5000 пристроїв, тоді необхідна лише одна ліцензія MM-VA-5K, а для управління бездротовою локальною мережею можуть бути надані кілька VMM. Крім того, менші ліцензії MM-VA можна скласти для підтримки більшої кількості пристроїв на Mobility Master. Однак існує момент, де складання менших ліцензій може коштувати дорожче, ніж одна більша ліцензія MM-VA.

Ліцензії попередньо встановлені на апаратному Mobility Master, оскільки вони є апаратними приладами і вони не здатні складати ліцензії, що призводить до більших витрат на ліцензування. Наприклад, якщо розгортання має підтримувати до 5000 пристроїв, тоді знадобляться два прилади MM-HW-5K, хоча разом вони досі будуть підтримувати лише до 5000 пристроїв.

Для всіх інших ліцензій (AP, PEF, RFP тощо) потрібно придбати необхідну кількість ліцензій, а база даних ліцензування буде поділена між декількома Mobility Master.

2.3.1 Приклади ліцензування

На даному етапі, хочу розповісти про приклади ліцензування, їх особливості та важливість використання цих ліцензій. В ArubaOS 8 існують такі типи:

- Зразок розгортання 1 - 800 точок доступу з ліцензіями AP, PEF, RFP, котрі керуються апаратними MC та віртуальними MM (VMM). За допомогою цього зразкового розгортання кожному з 800 точок доступу потрібно буде

мати ліцензію AP, PEF та RFP. Наявність VMM вимагає достатньої кількості ліцензій MM-VA, щоб охопити кожну точку доступу та MC під її управлінням. Ліцензія MM VA-1K надає пул з 1000 ліцензій. 800 з 1000 ліцензій у пулі споживаються точками доступу і це означає, що залишилось 200 ліцензій на покриття MC, а також на будь-яке майбутнє додавання пристроїв.

- Зразок розгортання 2 - 250 точок доступу з ліцензіями AP та PEF з використанням VMC та VMM. У цьому випадку ліцензія MM-VA 500 надає пул до 500 пристроїв на MM. Ліцензія MC-VA-250 дозволить використовувати до 250 точок доступу, що закінчуються на будь-якій кількості VMC під MM (це може бути один VMC або кілька VMC).
- Зразок розгортання 3 - 6000 точок доступу з ліцензіями AP, PEF та RFP з використанням апаратних MC та MM із надмірністю для кластеризації.
- Зразок розгортання 4 - 2000 точок доступу з ліцензіями AP, PEF та RFP, що підтримують 1500 клієнтів, які потребують VIA та криптографію Suite B, використовуючи апаратні MC та апаратні MM. Ліцензія MM-HW-5k надає пул для до 5000 пристроїв на MM.
- Зразок розгортання 5 - 2000 точок доступу з ліцензіями AP та PEF з використанням апаратних MC та HMM, що підтримують від 50 клієнтів на точку доступу до 10000 клієнтів. Кількість клієнтів набагато перевищує середню, тому загальна кількість точок доступу складає лише 2000, найбільший HMM повинен мати можливість розмістити всіх клієнтів.

До цих типів ще можна додати ліцензування автономних контролерів та ліцензування MCM.

MC Master (MCM) схожий на архітектуру контролера Master-Local в ArubaOS 6, де виділений спеціальний апаратний контролер служить центральним сервером ліцензування для всіх керованих локальних серверів та центральних пунктів конфігурації. Ліцензії можна налаштувати та встановити на контролер MCM. Пристрій (крім ліцензії MM-VA), Функції та ліцензії на основі сеансів повинні

масштабувати та використовувати однакові міркування на основі їх вимог до споживання (подібні до MM).

Однак ліцензії MC-VA для контролерів VMC, якими буде керувати MCM, будуть встановлені на окремі VMC, а VMC під MCM не можуть ділитися ліцензіями так, як це могло бути під управлінням Mobility Master.

Крім того, ліцензія MC-VA повинна бути встановлена і повинна відповідати платформі. Наприклад, єдину ліцензію MC-VA-250 не можна придбати та потім розділити на 5 VMC з 50 ліцензіями, спочатку MC VA-250 слід встановити на MC-VA-250 (або менший) VMC, яким не керує MM.

Щодо автономних контролерів, то під час його ліцензування, всі ліцензії на пристрій, функції та інші ліцензії, можуть бути встановлені на автономний контролер і споживатися таким же чином.

З ліцензії MC-VA на окремі контролери повинні встановлюватися в цілому і повинні відповідати платформі.

2.4 Кластеризація

Кластеризація - одна з особливостей, на яку треба звернути увагу в ArubaOS 8. Вона була розроблена, щоб скористатися архітектурою MM та придавати максимальну увагу до критично важливих мереж. Кластеризація розроблена, аби досягти наступних цілей:

- **Безшовне пересування** - клієнти в одному великому домені 2 рівня будуть асоціюватися та залашатись прив`язаними до єдиної MC під час руху (Рис. 2.10). Користувачі залишатимуться в одній підмережі та матимуть однакову IP-адресу, навіть якщо вони переміщаються між точками доступу з різних контролерів. Це забезпечує мобільність без ризику втратити продуктивність.
- **Резервний збій клієнта** - користувальницький трафік буде працювати безперебійно, а важливі сесії будуть збережені у випадку відмови одного

з членів кластера. Вплив на продуктивність буде пом'якшено настільки, що користувачі не помітять жодного погіршення їх роботи, і не знатимуть, що існує несправність незалежно від програм, які вони використовують.

- **Точка доступу та балансування навантаження клієнта** - точки доступу та користувачі автоматично балансують навантаження контролерів, які є членами кластера (Рис. 2.9). Цей процес забезпечує рівномірний розподіл з метою доставки і підтримки оптимальної продуктивності мережі та утримання потужності по всім членам кластеру для нових звя`зків між клієнтами.
- **Оновлення в режимі реального часу** - Aruba дозволяє клієнтам виконувати оновлення кластера, що дозволяє впроваджуватись новим функціям не впливаючи на продуктивність під час роботи мережі.

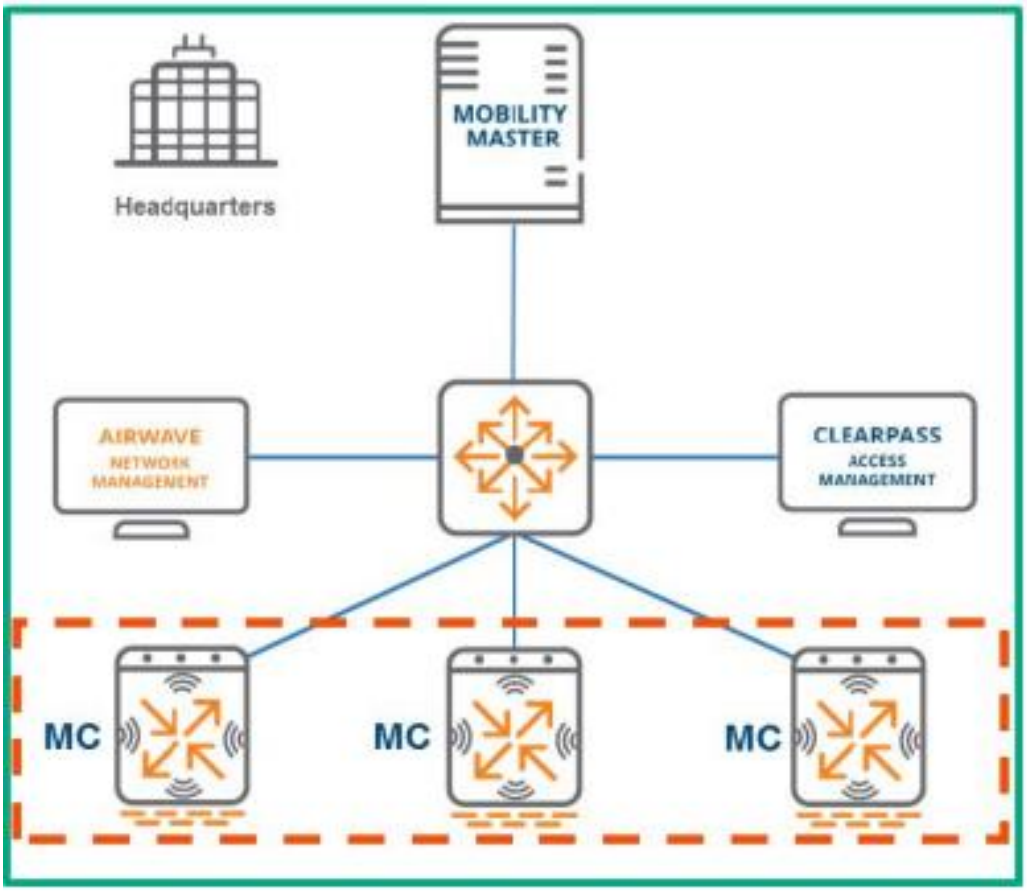

Рис. 2.9. Архітектура кластера MC

2.4.1 Формування кластера

Формування кластера включає в себе, так званий, процес рукостискання, коли повідомлення передаються через всіх потенційних членів кластеру. Цей процес відбувається за допомогою hello-повідомлень, якими обмінюються для перевірки рівня 3 між усіма членами кластера. Інформація, що стосується кластеризації, обмінюється через ці повідомлення, включаючи збірку, назву кластера та інформацію про MC, що надсилає повідомлення. Після всього, обмінявшись цими повідомленнями, члени кластера встановлять між собою зв'язок IPsec рівня 3 в повнозв'язну конфігурацію.

2.4.2 Ролі кластера

Контролер мобільності, окрім того, що є лідером кластера, може мати комбінацію наступних чотирьох ролей в кластері:

1. AP Anchor Controller (AAC)
2. User Anchor Controller (UAC)
3. Standby AAC (S-AAC)
4. Standby UAC (S-UAC)

AP Anchor Controller (AAC) можна розглядати як LMS для будь-якої AP, яка до нього прикріплена. Кожен AP отримає IP-адресу LMS, і як тільки вони будуть припинені, вони залишаться прив'язаними поки лідер кластеру визначить, що їх слід перемістити до іншого члена кластера. AP закріплений на своєму AAC у триступеневий процес:

- AP встановлює активні тунелі зі своїм AAC.
- Лідер кластера призначає резервний контролер AP (S-AAC) для одного з інших членів кластера.
- Після призначення точки доступу встановлюються резервні тунелі до S-AAC.

Щодо User Anchor Controller (UAC), концепція прикріплення користувачів до контролера за її допомогою є новою в ArubaOS 8 та була розроблена головним чином для покращення користувальницького досвіду роумінгу. Коли користувачі приєднуються до точки доступу, вони будуть використовувати існуючий тунель до свого UAC, якщо такий вже існує. Якщо AP не має тунелю до свого UAC, створюється динамічний тунель. Коли клієнт здійснює роумінг до нової точки доступу, то попередня точка доступу перетворюється в динамічний тунель. Користувальницький трафік завжди тунельно повертається до їх UAC, незалежно від того, який AP клієнт асоціюється з користувачем у роумінгу, навіть якщо ця точка доступу має інший AAC.

2.4.3 Функції кластеру

Найголовнішими функціями кластеру, котрі можна описати, є Seamless Roaming (Безшовне переміщення) та Stateful Failover (Резервний збій клієнта). Перевага UAC полягає в тому, що він значно покращує досвід для користувачів в межах кластера. Як тільки користувач приєднується до точки доступу, він хешує MAC-адресу клієнта та присвоює їй UAC. Тепер трафік від цього користувача завжди буде тунельований до його UAC. Це так і залишиться незалежно від того, до якої точки доступу користувачі приєднуються під час їхнього пересування, навіть якщо ця точка детермінуєтсья на іншому контролері.

Будь-яка точка доступу, до якої переходить користувач, автоматично перенаправить трафік на UAC, котрий буде призначений користувачеві. Якщо між UAC та точками доступу, між якими пересувається користувач, не існує активного тунелю або тунелю очікування, тоді буде створений динамічний тунель.

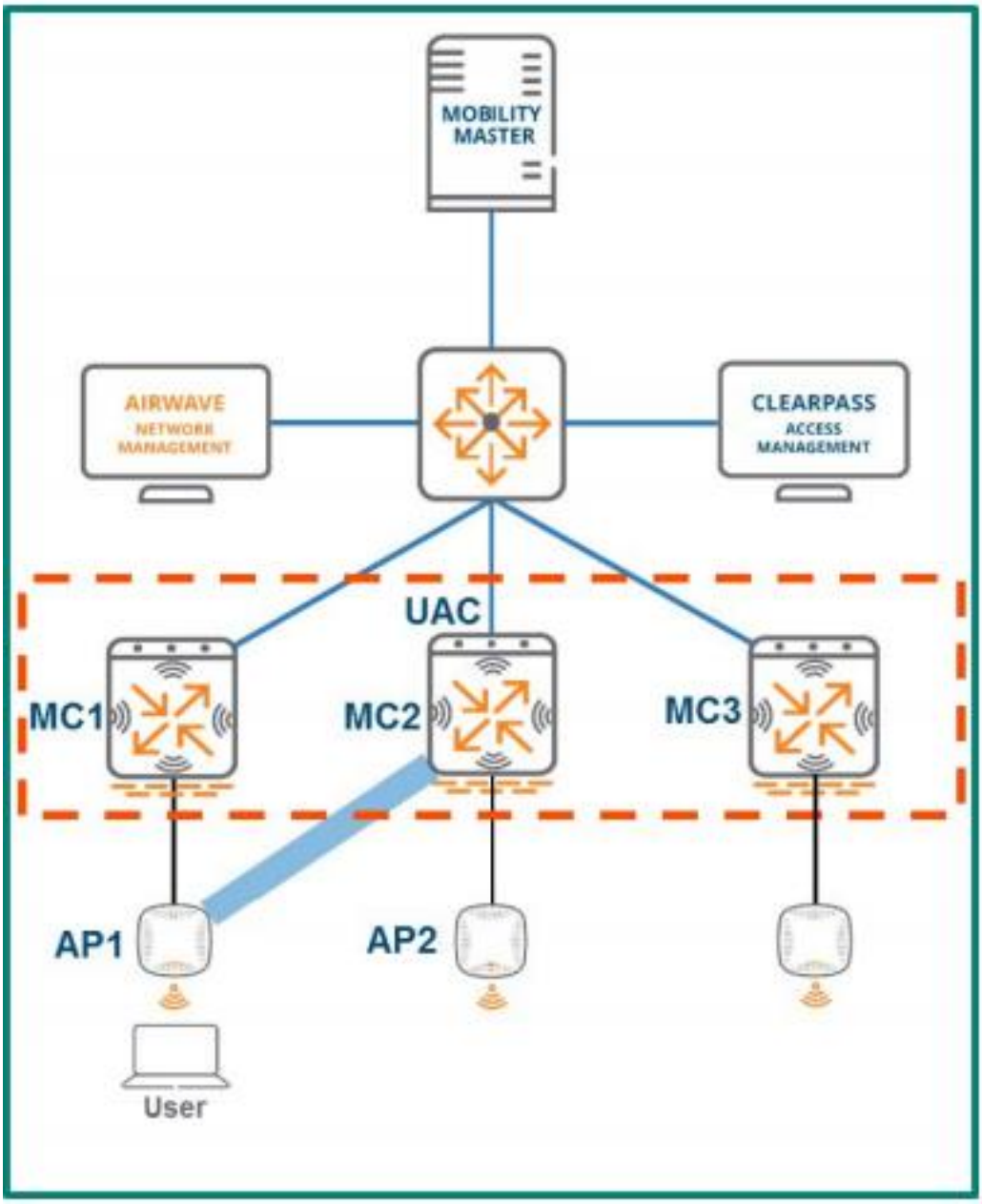

Рис. 2.10. Безшовне пересування кластеру

Stateful Failover - критичний аспект кластерних операцій, який захищає користувачів від будь-яких проблем, зв’язаних з відмовою контролера. Наступні дві ключові умови повинні бути виконані, щоб увімкнути цю функцію:

- Потрібно ввімкнути режим резервування. Його можна відключити, проте він увімкнений за замовчуванням.
- Між усіма членами кластера повинен існувати стан L2-Connected.

Якщо ці дві умови були виконані, стан клієнта буде повністю синхронізовано між UAC та S-UAC, це означає, що така інформація, як таблиця користувачів, стан layer 2 та layer 3 користувача, кеш ключа і кеш PMK будуть спільно використовуватися між обома пристроями. Крім того, такі сесії, як FTP та DPI-сесії, також синхронізуються з S-UAC. Синхронізація всього стану клієнта та інформація про сеанси високої цінності дозволяє S-UAC взяти на себе роль нової UAC клієнта, якщо поточний UAC користувача видає помилку. На рисунку нижче (Рис. 2.11) представлені переваги між L2-Connected та L3-Connected.

L2-Connected	L3-Connected
APs and clients are fully replicated	Only APs fully replicated
Users fully synced between nodes	Users not synced
High value sessions are synced	High value sessions not synced
Users failover with no de-auth	Users are de-authenticated upon failover
Fully redundant	Not fully redundant

Рис. 2.11. Переваги між станами L2-Connected та L3-Connected

Тут ми бачимо, що у L2-Connected точки доступу повністю копіюються разом з клієнтом, коли у L3-Connected копіюються лише точки доступу. Також у L2-Connected, на відміну від L3-Connected, користувачі синхронізуються між вузлами та синхронізуються головні сесії.

Кластери в операційній системі ArubaOS 8 дуже важливі гвинтики у механізмі роботи усієї системи, хоч і не помітні неозброєним оком для користувача, а сама кластеризація, як функція усієї операційної системи, являється одною з особливостей ArubaOS 8, що розділяє множини на підмножини, тим самим роблячи користування системою ще зручнішою та практичнішою.

3 ОСОБЛИВОСТІ РОБОТИ НОВИХ ФУНКЦІЙ В ARUBA OS 8

Коли був представлений AOS 8, його описали як абсолютно нову архітектуру. Операційна система Aruba була розроблена з нуля. Існують деякі подібності в графічному інтерфейсі та командному рядку, але відбулися суттєві зміни, які роблять цю нову архітектуру набагато вищою щодо масштабованості та надмірності.

3.1 Уніфікована комунікація та поєднання

Уніфікована комунікація та поєднання (UCC) - термін на Арубі, що описує інтеграцію служб корпоративного зв'язку в режимі реального часу, таких як обмін миттєвими повідомленнями, голос, відеоконференції, спільний доступ до робочого столу, спільний доступ до програм тощо. У контексті UCC як функція контролерів Аруби , комутатори та точки доступу, він представляє уніфікацію різних аспектів програм корпоративного спілкування та спільної роботи. Ці аспекти можна вільно класифікувати як виявлення засобів масової інформації, встановлення пріоритетів для засобів масової інформації та трафіку, моніторинг та видимість та класифікацію засобів масової інформації. Контролери Aruba підтримують такі програми UCC:

- Skype для бізнесу;
- Cisco Jabber;
- Протокол ініціювання сеансу (SIP);
- Виклики Wi-Fi.

Можливості функцій UCC не змінилися від ArubaOS 6, а UCC - це не нова функція в ArubaOS 8. Однак в ArubaOS 8 змінено архітектуру функції та спосіб її розгортання.

UCC складається з механізму глибокої інспекції пакетів (DPI), який працює на локальних контролерах в ArubaOS 6 і на контролерах мобільності в ArubaOS 8.

У ArubaOS 6 як DPI, так і UCC процеси запускаються на самих локальних контролерах. В ArubaOS 8 частина процесів UCC, які Аруба називає службою UCC або додатком UCC, була переміщена до Майстра мобільності, функціональність DPI залишається на контролерах мобільності.

Незважаючи на те, що UCC в ArubaOS 6 працює добре, є кілька недоліків у його конструкції, які були вдосконалені в ArubaOS 8, і це забезпечує наступні переваги для адміністраторів щодо міграції на ArubaOS 8:

- Відсутність видимості - в ArubaOS 6 видимість UCC не є централізовано на головному контролері. Статистика та моніторинг ведуться на місцевих контролерах. Ця конструкція не є ідеальною, оскільки вимагає, щоб користувачі входили в кожен локальний контролер окремо для моніторингу даних UCC.
- Складні оновлення - Додавання підтримки для нових додатків в ArubaOS 6 передбачає повне оновлення контролера, яке може спричинити загрозу для мережі.
- Відсутність агрегації SDN - використання API для програмного забезпечення, визначеної мережею Skype (SDN), в ArubaOS 6 передбачає налаштування SDN Manager з IP-адресами всіх абонентів у мережі. Це негативно впливає на масштабованість мережі.

На відміну від цього, ArubaOS 8 вирішує перераховані вище завдання, покращуючи функціональність у цілому, завдяки своєму чудовому архітектурному дизайну та підходу до впровадження UCC. UCC тепер працює як додаток (або завантажувана послуга) на Mobility Master. Механізм DPI продовжує працювати на контролерах мобільності, які функціонують як локальні контролери в ArubaOS 6. Класифікація та визначення пріоритетів функціональних можливостей прийняття рішень було переміщено до Mobility Master разом із шлюзом рівня додатків VoIP, який працює як частина програми UCC. Крім того, функцію UCC можна оновити незалежно, не потребуючи оновлення всіх контролерів у мережі, оскільки це один із LSM.

Цей безперешкодний процес оновлення дозволяє адміністраторам додавати підтримку нових голосових програм та програм UCC, не зазнаючи жодних негативних наслідків, пов’язаних із перезавантаженням контролера. Mobility Master пропонує важливу цінність для підприємств, які використовують SfB як свою програму UCC. API SfB SDN тепер можна агрегувати в Mobility Master для всіх контролерів мобільності. Це позбавляє від необхідності налаштовувати менеджер SDN SDB на тисячі IP-адрес окремих абонентів. Майстер мобільності відстежує контролер мобільності та те, де було ініційовано виклик, і узгоджує повідомлення SDN API, отримані від менеджера SDN SDN, із потоками викликів під час програмування шляху даних на цьому конкретному контролері мобільності.

Застосування архітектури, заснованої на Mobility Master, представлено в ArubaOS 8, яка забезпечує централізований огляд UCC через WebUI Mobility Master.

3.2 Оптимізації безпроводової мережі на основі Aruba AirMatch

AirMatch забезпечує безпрецедентну якість розподілу ресурсів мережі RF. Він збирає дані статистики радіочастотної мережі за останні 24 години і активно оптимізує мережу на наступний день. Необхідно впроваджувати зміну плану радіочастот під час мінімального використання мережі, щоб відключення клієнтів надавало мінімальний вплив на взаємодію з користувачем. На додаток до планування каналів, що виконується кожні 24 години, AirMatch також реагує на динамічні зміни в радіочастотному середовищі, такі як радар і події з високим рівнем шуму. AirMatch забезпечує стабільну роботу мережі зі значно мінімальнішою зміною каналу та EIRP. AirMatch визначається наступними ключовими атрибутами:

- Централізована служба оптимізації радіочастотного сигналу;
- Нові шляхи збору інформації та розгортання конфігурації ;

- Моделює і вирішує мережу в цілому ;
- Результати в оптимальному каналі, смузі пропускання і плані EIRP для мережі.

До речі, слід помітити, що AirMatch функціонує лише в тому випадку, якщо мережею керує MM та несумісна з архітектурою MCM. У топології MCM усі рішення про оптимізацію каналів, пропускну здатність, EIRP та інші RF будуть і надалі приймати ARM, як це було б в архітектурі ArubaOS 6.

Якщо зв'язок між Mobility Master і контролером мобільності знизиться, Mobility Master буде недосяжним, і це матиме вплив на продуктивність. Однак AirMatch все ще буде функціонувати. Найголовніше те, що функції, які вимагають централізованої координації Mobility Master, будуть втрачені, такі як заплановані оновлення для оптимізації радіочастот. Поточне радіочастотне рішення продовжуватиме функціонувати, і все одно відбуватимуться зміни, спричинені подіями з високим рівнем шуму та радіолокацією.

Насправді, AirMatch - це послуга автоматичного радіочастотного планування Аруби наступного покоління, яка призначає канали, пропускну здатність та потужність радіостанціям у всій мережі. Служба AirMatch працює на Mobility Master і генерує RF-рішення, яке визначає нові канали, пропускну здатність та налаштування EIRP для кожного радіо. Робочий процес AirMatch відбувається за допомогою наступних кроків:

1. Точки доступу надсилають статистику RF як повідомлення AMON контролерам мобільності.

2. Контролер мобільності пересилає повідомлення AMON своєму Mobility Master.

3. AirMatch розраховує оптимальне радіочастотне рішення.

4. Mobility Master відтісняє рішення назад до контролерів мобільності.

5. Контролер мобільності відправляє радіопрофілі dot11 в точки доступу.

3.3 Класифікація веб-вмісту

Класифікація веб-вмісту (WebCC) - це функція на контролерах Аруби та IAP, яка була вперше представлена в ArubaOS 6. Вона класифікує трафік http і https за категоріями та репутацією. Потім, правила брандмауера можуть бути застосовані відповідно до класифікації WebCC. Це запобігає шпигунському та шкідливому програмному забезпеченню, блокуючи доступ до небезпечних та забезпечуючи видимість категорій веб-вмісту та веб-сайтів, до яких користувачі отримують доступ. У розгортанні ArubaOS 6 процес WebCC працює на локальних контролерах. В ArubaOS 8 основна архітектура була змінена шляхом переміщення процесу WebCC до Mobility Master у вигляді програми або завантажуваної послуги.

Наприклад, в ArubaOS 6 WebCC працює як процес на локальних контролерах і працює спільно з шляхом до даних. Його основна роль полягає в тому, щоб відстежувати трафік http / https у шляху до даних та перевіряти його, щоб визначити, чи потрібні подальші дії. Як тільки клієнт має IP-зв'язок і отримує доступ до URL-адреси, шлях даних перехоплює трафік http (-ів) від клієнта та перевіряє відповідність його локального кешу URL-адрес. Якщо datapath знаходить збіг, застосовуються правила класифікації та репутації.

Класифікація, надана WebCC, також використовується у списку доступу до брандмауера, який може вжити заходів, щоб дозволити або заборонити доступ до URL-адреси на основі додаткової інформації. Якщо кеш шляху до даних не знаходить збігу з URL-адресою, до якої намагається отримати доступ клієнт, тоді тригер URL-пропуску надсилається до WebCC. Процес WebCC шукає URL-адресу в базі даних, що підтримується контролером. Якщо знайдено збіг, URL-адреса буде класифікована, а інформація буде надана в шлях до даних. Потім ця інформація використовується в ACL, щоб заборонити або дозволити доступ до URL-адреси. Якщо процес WebCC не знаходить збігу в базі даних URL-адрес, він виконує хмарний пошук у реальному часі зі сховища Brightcloud і запитує класифікацію URL-адреси.

Хоча WebCC в ArubaOS 6 пропонує суттєві переваги, у дизайну є кілька недоліків. Кожен контролер підтримує базу даних URL-адрес, однак розміри

контролерів різняться, як і їх база даних та обсяг пам'яті. База даних веб-URL, яку можна підтримувати на контролері, залежить від розміру цього контролера. Імовірність знайти URL-адресу в локальній базі даних зменшується в міру зменшення розмірів контролерів. Це призводить до збільшення кількості випадків, коли для класифікації URL-адрес у випадку пропуску URL-адреси потрібен хмарний пошук у реальному часі. Також збільшується час, необхідний для блокування URL-адреси, що дозволяє користувачам отримати доступ до URL-адреси, яку слід було заблокувати. Іншим недоліком WebCC в ArubaOS 6 є те, що кожен локальний контролер повинен індивідуально зв’язуватися з Brightcloud. Крім того, локальні контролери споживають пам’ять і простір для підтримки своєї бази даних URL.

В свою чергу, зміни дизайну WebCC в ArubaOS 8 дають численні переваги порівняно з недоліками, властивими дизайну WebCC в ArubaOS 6:

- WebCC працює як завантажуваний сервісний модуль Mobility Master.
- Контролери мобільності підтримують лише неглибокий кеш URL-адрес, що економить пам'ять.
- Mobility Master має більшу пам’ять і здатний підтримувати базу даних URL-адрес із до 1 мільйона записів.
- Хмарний пошук для пропущеної URL-адреси виконує лише Mobility Master.

Хоча потік WebCC в ArubaOS 8 схожий на ArubaOS 6, є кілька ключових відмінностей, на які слід звернути увагу. Найважливіша відмінність полягає в тому, що процес WebCC в ArubaOS 8 (Рис. 3.1) працює на Mobility Master замість контролера мобільності.

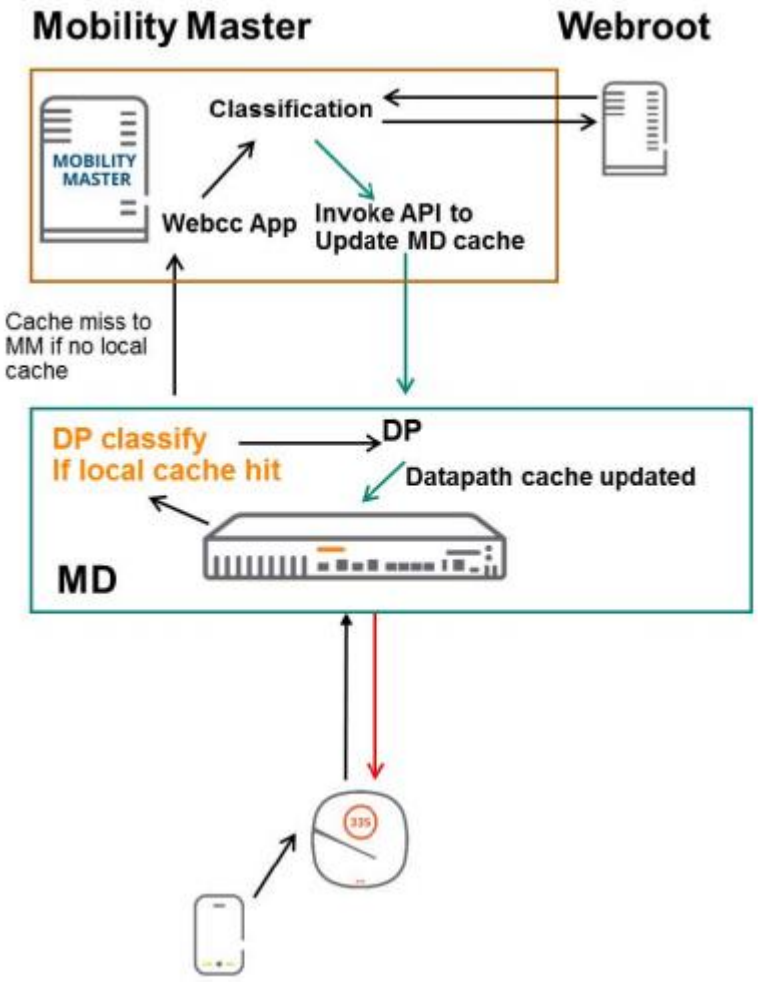

Рис. 3.1. WebCC в ArubaOS 8

На відміну від AOS 6, в AOS 8, коли користувач намагається отримати доступ до URL-адреси http або https, пакет переглядається шляхом передачі даних на контролері мобільності, який підтримує локальний кеш URL-адрес. Якщо URL-адресу знайдено в локальному кеші контролера мобільності, застосовується класифікація, і можна вжити подальших дій, щоб дозволити або заборонити доступ на основі будь-яких налаштованих ACL. Якщо шлях даних контролера мобільності не знаходить URL-адресу у своєму локальному кеші, тоді спрацьовує промах URL-адреси та надсилається до Майстра мобільності. Mobility Master шукає URL-адресу у своїй базі даних, яка значно більша, ніж локальний кеш на контролері мобільності. Якщо знайдено збіг, результат класифікації буде відправлений назад до контролера мобільності, який визначить, чи потрібно вживати дії для обмеження доступу чи не на основі існуючих ACL. Якщо Mobility

Master не знаходить відповідності у своїй локальній базі даних, він виконує хмарний пошук через Webroot. Mobility Master оновить свій локальний кеш і шлях даних контролера мобільності, який ініціював запит пошуку.

3.3 Нові можливості організації користувачів на базі Aruba AirGroup

AirGroup являється компонентом ArubaOS, який вирішує проблеми юзабіліті та продуктивності, пов'язані з використанням служб багатоадресної системи доменних імен (mDNS) у корпоративних та освітніх мережах.

Мережеві служби з нульовою конфігурацією, такі як Bonjour та інші служби mDNS, виявляють, призначають адреси та роздільну здатність імен для настільних комп’ютерів, мобільних пристроїв та мережевих служб. Вони розроблені для плоских IP-мереж з однією підмережею, таких як розгортання житла. У великих університетах та корпоративних мережах пристрої, що підтримують Bonjour, часто підключаються до мережі через VLAN. Як результат, користувацькі пристрої, такі як iPad на певній VLAN, не можуть виявити Apple TV, який знаходиться в іншій VLAN. Для того, щоб використовувати послуги mDNS на мобільних пристроях у корпоративному середовищі, AirGroup управляє багатоадресними мережевими багатоадресними передачами з нульовою конфігурацією, щоб покращити пропускну здатність мережі, спростити підключення до пристроїв, які відповідають користувачеві та місцезнаходженню, та належним чином переадресовувати через підмережі.

Наприклад, в ArubaOS 6, протокол mDNS призначений для полегшення багатоадресного зв'язку та добре працює в межах L2. Однак лише пристрої, що підтримують mDNS, в одній і тій же VLAN можуть взаємодіяти між собою. Наприклад, iPad у VLAN 10 не може взаємодіяти з Apple TV у VLAN 20. Аруба створила AirGroup, щоб полегшити зв’язок між пристроями через VLAN та забезпечити фільтрацію однорангового багатоадресного трафіку на основі атрибутів, включаючи VLAN, роль користувача, ім'я користувача, група користувачів та місцезнаходження. Кожен контролер створює таблицю кешу

mDNS, вивчаючи та припиняючи запити та рекламу mDNS або Digital Living Network Alliance (DLNA) по повітрю. Наприклад, щоразу, коли iPad надсилає запит AirPlay, контролер переглядає свою таблицю кешу mDNS, і якщо служба AirPlay доступна, він реагує на iPad за допомогою одноадресного передавання. Одноадресні пакети допомагають зменшити використання каналу в повітрі.

Домени AirGroup можна використовувати для зв'язку mDNS та DLNA між пристроями через різні контролери. Крім того, контролери здатні інтегруватися з ClearPass для створення персональних мереж. Сервери AirGroup можна визначити на ClearPass і, за бажанням, спільно використовувати їх разом з іменами користувачів, ролями користувачів, групами користувачів, групою точок доступу, назвою точки доступу та AP FQLN.

Хоча AirGroup в ArubaOS 6 здатний забезпечити значні покращення функціональності, він страждає від обмежень масштабованості. ArubaOS 8 вирішує питання масштабованості платформи AirGroup в ArubaOS 6, де масштабованість була обмежена можливостями платформи контролерів.

На відміну від ArubaOS 6, де кожен контролер запускає AirGroup окремо, функціонал AirGroup було переміщено до Mobility Master в ArubaOS 8. Вся таблиця кеш-пам'яті mDNS розташована на Mobility Master. Контролер OpenFlow встановлений на Mobility Master, а агенти OpenFlow встановлені на контролерах мобільності для передачі інформації mDNS та DLNA. Кожного разу, коли контролери мобільності перехоплюють запит або рекламу mDNS або DLNA, вони передаються до Mobility Master за допомогою каналу OpenFlow. Mobility Master створює відповідні потоки mDNS / DLNA на основі своїх політик AirGroup і спрямовує ці потоки до контролерів мобільності. Контролери мобільності дозволяють або забороняють зв'язок mDNS та DLNA для пристроїв AirGroup у WLAN. AirGroup значно більш масштабована в ArubaOS 8, оскільки Mobility Master оснащений відповідними ресурсами для обробки великих обсягів зв'язку mDNS в мережі порівняно з апаратним контролером в ArubaOS 6.

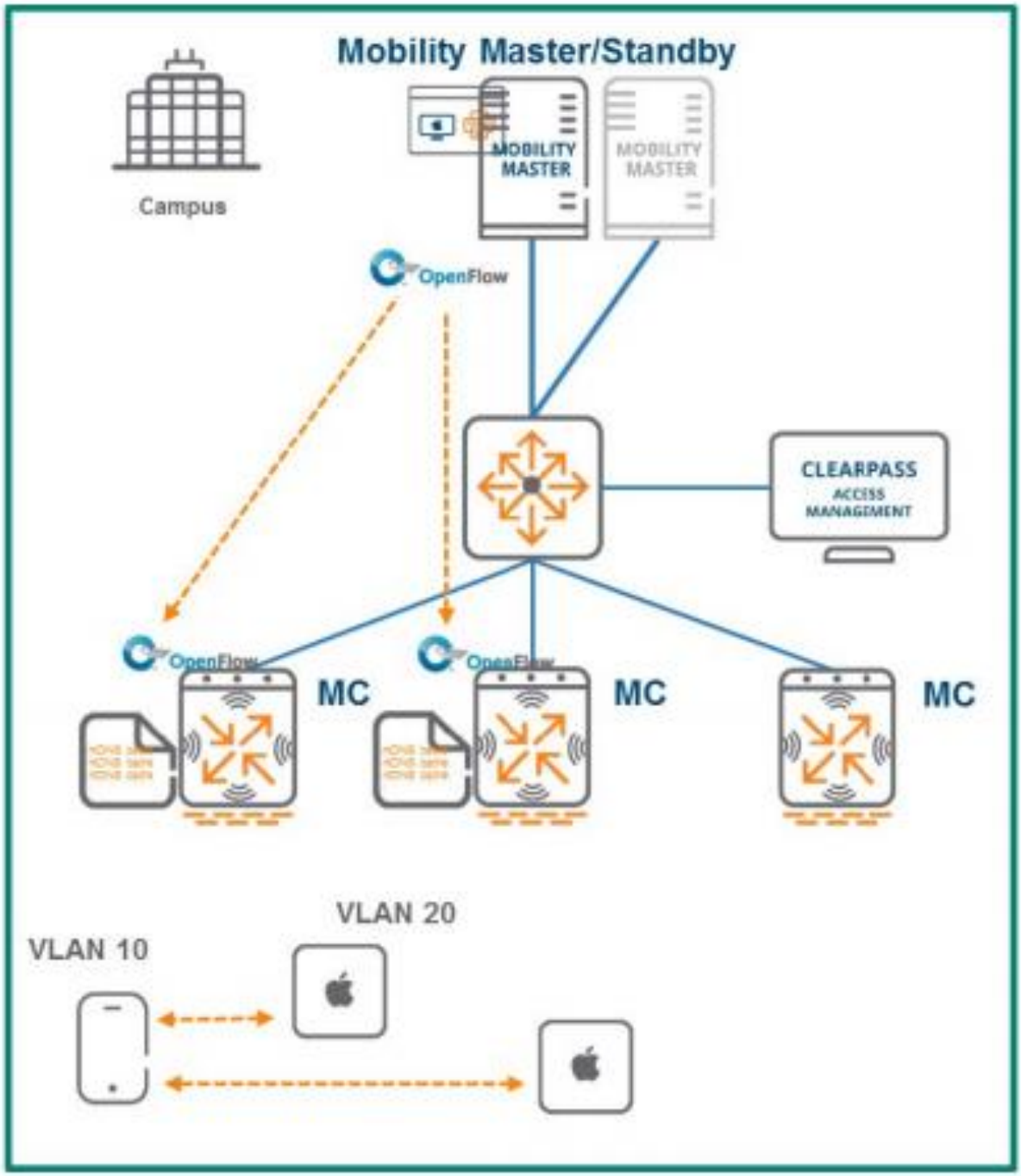

Рис. 3.2. AirGroup в ArubaOS **8.**

3.4 Підвищення продуктивності Web-трафіку за допомогою ArubaAppRF

AppRF в ArubaOS 6 має можливість ідентифікувати та застосовувати політики приблизно до 2000 додатків, включаючи дозволи, блокування або обмеження швидкості. Оновлення AppRF або додавання нових підписів AppRF в

ArubaOS 6 вимагає системного оновлення. Наприклад, навіть якщо нові підписи потрібно протестувати лише на одному з локальних контролерів або виправити помилку під час розгортання контролера Master-Local, головний контролер у мережі потрібно оновити разом із усіма локальними контролерами. Це обмеження спричиняє порушення мережі та вимагає планування простоїв для всієї мережі. Крім того, ArubaOS 6 не може створювати власні політики AppRF або власні категорії програм.

ArubaOS 8 забезпечує підтримку додавання нових програм до контролера без необхідності виконувати оновлення. Набір прото можна завантажити та активувати під час виконання, щоб додати підтримку нових програм. На даний момент DPI підтримує близько 2000 програм, до яких можуть застосовуватися правила. В ArubaOS 6 спеціальні програми, такі як внутрішні для організації програми, не можна класифікувати.

ArubaOS 8 підтримує спеціальні програми, які можна надсилати до контролерів мобільності за бажанням. Нові програми, визначені на Mobility Master, зберігатимуться як підписи додатків у двійковому форматі та доставлятимуться до контролерів мобільності, коли конфігурації будуть натискатися вниз. Потім підпис програми додається до активного набору підписів на контролері мобільності, що забезпечує підтримку та визначення нових програм за потреби. Mobility Master може налаштувати до 64 користувацьких програм із 16 правилами для кожної програми. Також можна створювати власні категорії програм і застосовувати до них політику. Навіть якщо контролер мобільності втрачає зв’язок із Mobility Master та резервним Mobility Master, він не втратить функціональність класифікації програм.

Як ми бачимо, функція AirGroup управляє багатоадресними мережевими багатоадресними передачами з нульовою конфігурацією, щоб покращити пропускну здатність мережі , AirMatch забезпечує стабільну роботу мережі зі значно мінімальнішою зміною каналу, а AppRF роблять користування ArubaOS 8 лише зручніше та виконує такі задачі, котрі не виконувала ArubaOS 6.

ВИСНОВОК

Розглянуті у роботі методи розгортання безпроводових мереж, допомагають організаціям створювати надійні системи, котрі дають змогу покрити мережею усю потрібну територію. За допомоги операційної системи ArubaOS 8 робота бездротових мереж стає більш надійною, завдяки новим функціям, котрих не було у попередній версії ArubaOS 6. Вони допомагають налаштувати систему, котра буде зручною у використанні, працездатною та, найважливіше всього, захищеною. Тому для цього, Mobility Master має бути повністю налаштований адміністратором мережі, подібно до того, як головний контролер має бути налаштований в ArubaOS 6. Основна роль Mobility Master полягає в тому, щоб служити єдиною точкою конфігурації та управління зображеннями для мережі. Кластеризація є одною з особливостей, на яку треба звернути увагу в ArubaOS 8. Вона була розроблена, щоб скористатися архітектурою ММ та придавати максимальну увагу до критично важливих мереж.

Використовуючи усі перераховані функції вище, відкривається можливість створити відмінну, від інших, мережу, на котру не потрібно витрачати багато сил. На мою думку, операційна система ArubaOS 8 є, якщо не єдиною, то одною з найкращих для створення безпроводових мереж.