Лабораторна робота №4. Налагодження та дослідження роботи бездротової локальної мережі побудованої з використанням бездротових контролерів Cisco

Мета роботи: ознайомитися з особливостями функціонування та налагодження роботи бездротової локальної мережі WLC; ознайомитись з SSID та VLAN конфігурації на WLC та з автоматичною реєстрацію точок доступу Light Weight.

Теоретичні відомості

Загальні теоретичні відомості про Wireless Lan Controller – WLC

WLC (*Wireless Lan Controller*) – це пристрій, який дозволяє централізовано керувати бездротовими мережами, забезпечуючи ефективну роботу точок доступу (AP), моніторинг трафіку, управління безпекою і політиками доступу для користувачів. WLC дозволяє полегшити адміністрування, оскільки всі налаштування, оновлення та моніторинг виконуються через єдиний контрольний пункт. Це рішення підходить для великих підприємств, кампусів та організацій, які потребують масштабованої, надійної та безпечної бездротової інфраструктури. Завдяки таким функціям, як підтримка сучасних стандартів Wi-Fi (802.11ac, 802.11ax), автоматичне налаштування точок доступу, моніторинг спектра та захист від завад, Cisco WLC забезпечує високу продуктивність і стабільність бездротового зв’язку.

В даний час Cisco пропонує ряд різних моделей WLC, кожна з яких орієнтована на різні мережі. Зокрема, моделі для корпоративного сектору (WLC 8500, 7500, 5760 та ін.), зображені на рис. 7.1, пропонують більше високошвидкісних мережевих інтерфейсів гігабітного типу, високу доступність та деякі розширені функції, необхідні у великих та складних мережах, наприклад, підтримка більшої максимальної кількості VLAN та Wi-Fi-мереж, тисячі точок доступу для клієнтів на WLC-пристрої та багато іншого.

Останнім часом компанія Cisco почала пропонувати WLC-функціонал у комутаторах серії Catalyst шляхом вбудовування WLC всередині Catalyst Switches, наприклад Catalyst 3850, а також як віртуальний образ Virtual WLC, який працює під VMware ESX / ESXi 4.x / 5.x.

Маршрутизатори Cisco ISR G2 Series 2900 і 3900 підтримують модулі серверу Cisco UCS-E, додаючи функціональність WLC, підтримуючи до 200 точок доступу та 3000 клієнтів.

Рисунок 7.1 – Види моделей Wireless Lan Controller

Загальна характеристика одного із видів WLC 2504

Контролер 2504 працює у поєднанні з легкими точки доступу Cisco та системою бездротового керування Cisco (WCS) для забезпечення системних функцій бездротової локальної мережі. Як компонент уніфікованої бездротової мережі Cisco (CUWN), контролер 2504 забезпечує взаємодію в реальному часі між точкою доступу бездротового зв'язку та іншими пристроями для надання централізованої політики безпеки, гостьового доступу, системи захисту від бездротового вторгнення (WIPS), контекстно), нагороджена організація управління, якість послуг для мобільних послуг, таких як голос і відео, та підтримка OEAP для рішення Teleworker.

Контролери 2504 підтримують до 50 легких точок доступу з кроком 5 точок доступу з мінімум 5 точок доступу, що робить його економічним рішенням для роздрібної торгівлі, філій підприємств та малого та середнього бізнесу. Контролер 2504 поставляється з чотирма 4 Gigabit Ethernet портами.

Контролер 2504 забезпечує надійне покриття 802.11 a / b / g і забезпечує безпрецедентну надійність, використовуючи 802.11n за допомогою бездротових рішень Cisco Next-Generation і Wireless Mesh Cisco.

На рис. 7.2 – продемонстрована мережева топологія та мережеві підключення контролера 2504, яка показує необхідні кабелі Ethernet для середовища, залежного від інтерфейсу (MDI). Контролер має функцію автоматичного MDI, тому ви можете використовувати прямі або перехресні кабелі.

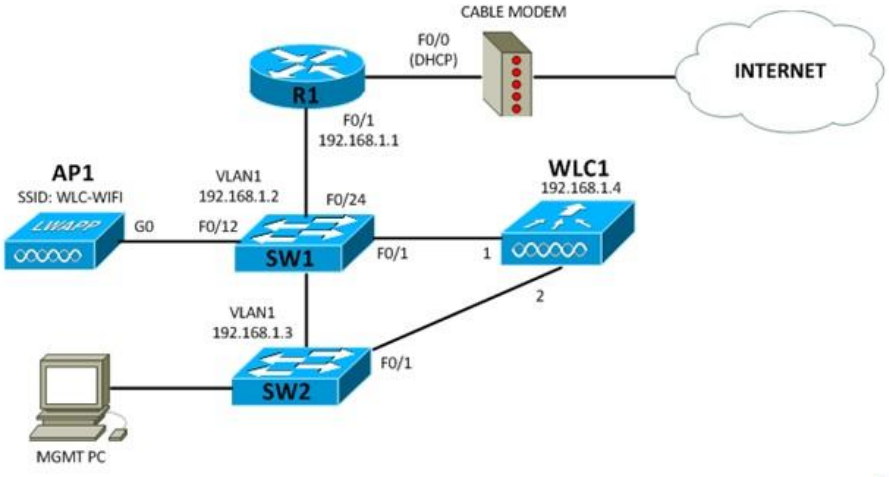

Рисунок 7.2 – Типова топологія та мережеві підключення

Загальна характеристика одних із видів WLC, серії 7500 та 8500

Бездротовий контролер серії Cisco 7500 – це високопродуктивне рішення для управління бездротовими мережами підприємств, яке дозволяє централізовано керувати доступом до Wi-Fi для великої кількості точок доступу (Access Points, AP) в середніх та великих організаціях (рис. 7.3). Ця модель контролера була представлена компанією Cisco як частина її портфеля рішень для організаційного бездротового зв'язку. Контролер Cisco Flex 7500 може управляти бездротовими точками доступу у понад 500 відділеннях, що дозволяє IT-менеджерам налаштовувати, керувати та усувати помилки до 2 000 точок доступу та 20 000 клієнтів. Підтримка різних технологій безпеки, таких як WPA2, WPA3, 802.1X для автентифікації користувачів та захисту мережі від атак, зокрема, з використанням шифрування трафіку та контрзаходів для захисту від несанкціонованого доступу.

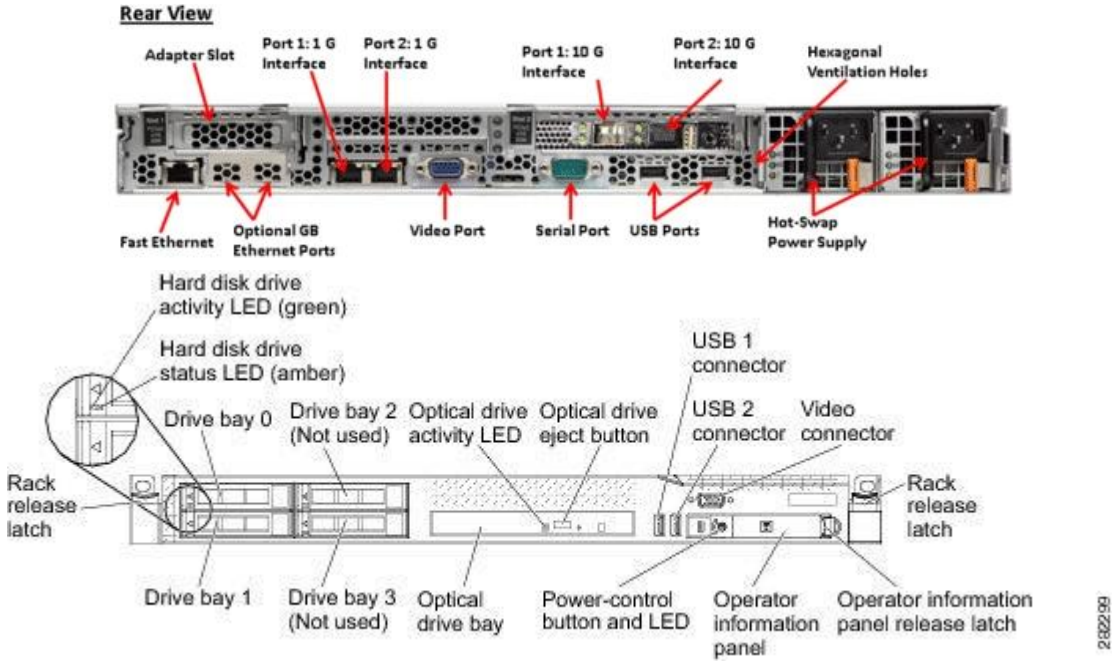

Рисунок 7.3 – Бездротовий контролер Cisco Flex 7500

Компоненти передньої панелі:

- засувки для рознімання: Натисніть засувки на кожній передній панелі контролера, щоб витягнути її зі стійки.

- світлодіоди стану жорсткого диску: Цей індикатор використовується для позначення стану жорстких дисків SAS. Коли цей світлодіод горить, це означає, що пристрій не працює. Коли цей індикатор мигає повільно (один спалах на секунду), це означає, що пристрій перебудовано. Коли світлодіод блимає швидко (три спалаха в секунду), це означає, що контролер ідентифікує привід.

- індикатор активності жорсткого диску: кожен жорсткий диск має індикатор активності, і коли цей індикатор блимає, це означає, що пристрій виконує операції із диском.

- кнопка виймання оптичного приводу: Натисніть цю кнопку, щоб

випустити DVD або компакт-диск із DVD-приводу.

- індикатор активності оптичного приводу: коли цей світлодіод горить, це означає, що DVD-привід використовується.

- панель інформації оператора: ця панель містить елементи керування та світлодіодні індикатори, які надають інформацію про стан контролера.

- засувка для зняття інформаційної панелі оператора: Посуньте синій фіксатор ліворуч, щоб витягнути панель діагностики та переглянути світлодіоди та кнопки діагностики.

- відео роз'єм: підключіть монітор до цього роз'єму. Відео роз'єми на передній і задній панелі контролера можуть бути використані одночасно. Конфігурація та керування контролером підтримується лише через підключення до послідовного інтерфейсу. Конфігурація та керування контролером не підтримується за допомогою клавіатури та монітора, безпосередньо підключених до контролера.

Однією з особливостей бездротового контролера Cisco Flex 7500 є модуль інтегрованого керування (IMM). IMM поєднує функції процесорів сервісу. IMM управляє сервіс-процесором, моніторами та сповіщеннями. Якщо стан навколишнього середовища перевищує порогову величину або якщо компонент системи не працює, IMM вимикає світлодіоди, щоб допомогти адміністратору діагностувати проблему, сповістити та записати помилку в журналі подій. IMM забезпечує керування віддаленим сервером за допомогою стандартних галузевих інтерфейсів: простий протокол керування мережею (SNMP) версії 3 – Web-браузер. Допомагає забезпечити безперервність роботи в кожній локальній мережі через відмову від помилок WAN. Ефективна мережа з локальним перемиканням трафіку даних дозволяє оптимізувати WAN та правила QoS, не вимагаючи тунелювання через WAN. Інші переваги контролера серії Cisco Flex 7500 включають:

- технологія Cisco CleanAir для самовідновлення автономної мережі, яка дозволяє уникнути перешкод у системі РЧ;

- Cisco ClientLink, для підвищення надійності та охоплення існуючих клієнтів;

- технологія Cisco ClientLink оптимізує бездротові мережі змішаного типу, допомагаючи гарантувати, що клієнти 802.11a / g та 802.11n працюють на максимально можливій швидкості.

Бездротовий контролер Cisco 8510 - це високопродуктивний контролер для управління бездротовими мережами, орієнтований на великі підприємства та організації, які потребують високої масштабованості та надійності бездротових рішень.

Контролер Cisco WLC 8510 є частиною серії Cisco 8500 і є однією з найбільш потужних моделей контролерів компанії для управління Wi-Fi мережами (рис. 7.4). Він пропонує функції для ефективного управління великою

кількістю точок доступу (AP) з великим числом клієнтів, а також має значну гнучкість у забезпеченні надійної роботи бездротових мереж.

Контролер Cisco 8510 може керувати централізованим (локальним режимом), режимом FlexConnect та розгортанням сітки в одному контролері.

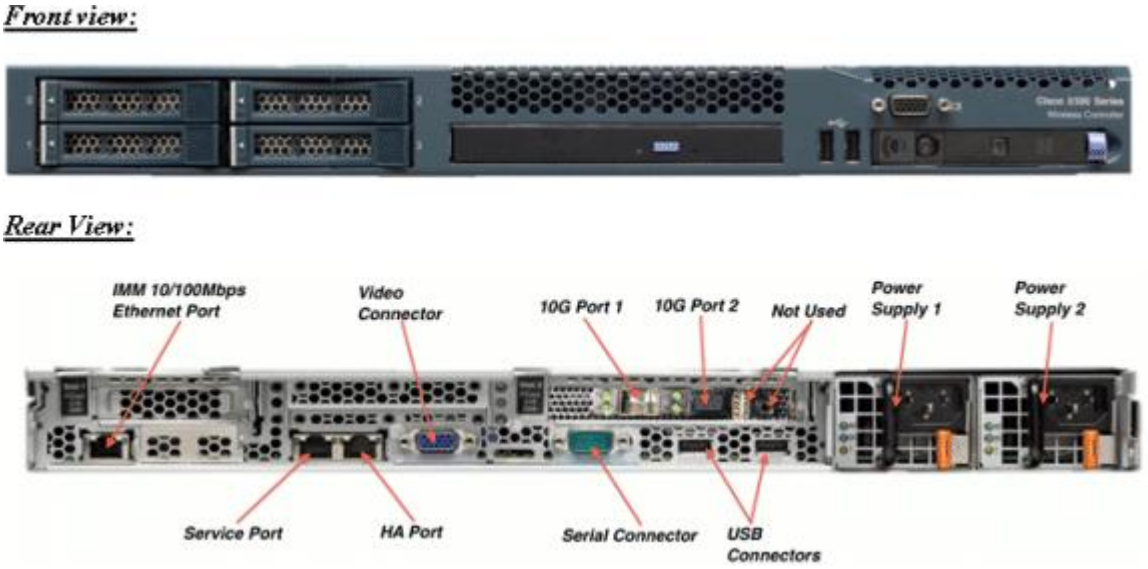

Рисунок 7.4 – Бездротовий контролер Cisco серії 8500 – 8510

Бездротовий контролер Cisco 8510 доступний у двох версіях: стандартній версії змінного струму з PID [AIR-CT8510-K9] та новою версією DC з PID [AIR-CT85DC-K9].

Єдина різниця між цими двома пропозиціями - це джерело живлення, яке постачається з продуктом. Деякими ключовими атрибутами контролера Cisco 8500 є:

- висока щільність клієнта;
- підтримка 6000 АП, 6000 груп АП, 2000 груп FlexConnect і до 100 АП на групу FlexConnect;
- підтримка 4096 VLAN;
- відстеження 50 000 радіочастотних ідентифікаторів, виявлення та обмеження до 24 000 шахраїв, а також до 32 000 шахраїв;
- HA з Sub-second AP Stateful Switchover;
- зовнішня підтримка;
- підтримка всіх режимів роботи AP (локальний, FlexConnect, монітор, детектор розвідників, Sniffer, та міст);
- підтримка High Availability (HA), що забезпечує безперервну роботу мережі у разі збоїв;
- WFA Passpoint Certified;
- 802.11r швидкий роумінг;
- підтримка Cisco Prime Assurance, що включає інструменти для діагностики проблем у мережі і моніторингу продуктивності;

- ліцензування права на використання (RTU) для полегшення нового ліцензування та виконання поточного;

Функції, які наразі не підтримуються платформою 8500

- локальна автентифікація (де Контролер діє як сервер автентифікації);
- внутрішній DHCP-сервер;
- Wired Guest;
- TrustSec SXP;

Контролер Cisco 8500 дозволяє за замовчуванням перескеровувати консоль із швидкістю 9600, що імітує термінал VT100 без керування потоком. Контролер 8500 має таку ж послідовність завантаження, як і інші контролери (рис. 7.5).

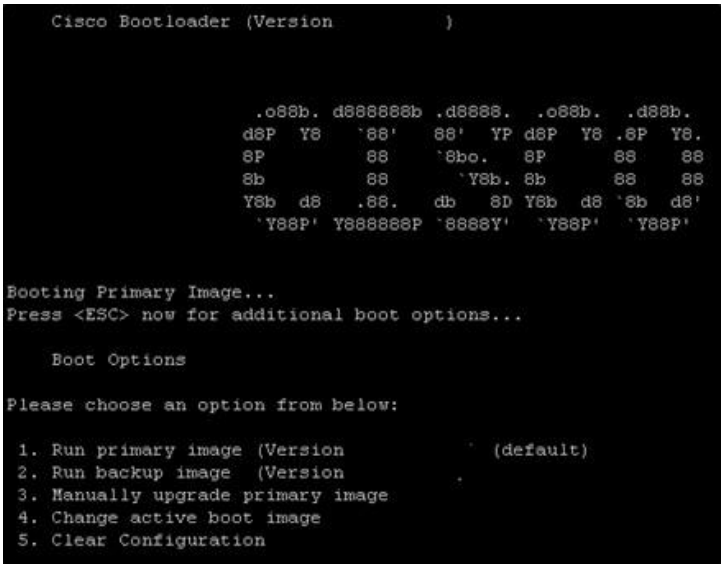

Рисунок 7.5 – Запуск бездротового контролера 8510

Загальні відомості про SSID та VLAN на WLC

Динамічні інтерфейси на Cisco Wireless LAN Controller (WLC) використовуються для розділення трафіку між різними типами мережевих зон, наприклад, для ізоляції трафіку користувачів, гостів, або для управління різними службами (наприклад, для передачі даних і голосового трафіку). Вони дозволяють створювати окремі логічні інтерфейси, які можуть бути асоційовані з конкретними VLAN (Virtual Local Area Network) і призначені для різних сегментів мережі, зокрема для підключення клієнтів до мережі. При підключенні клієнта до бездротової мережі, WLC автоматично призначає йому відповідний динамічний інтерфейс, залежно від політики, що визначена для відповідного SSID (службового імені мережі). Це забезпечує гнучкість та дозволяє ефективно керувати трафіком, а також підвищує безпеку, оскільки трафік для різних груп користувачів може бути ізольований і оброблений окремо.

Якщо порт неприєднаний, всі динамічні інтерфейси повинні бути розташовані в іншій IP-підмережі з будь-якого іншого інтерфейсу, налаштованого на порту. Інформацію про максимальну кількість VLAN-

серверів, що підтримуються на платформі Cisco WLC, див. у відповідній таблиці платформи Cisco WLC. Cisco рекомендує використовувати теговані VLAN для динамічних інтерфейсів. VLAN з контролерами WLAN використовують модель, зазначену на рис. 7.6:

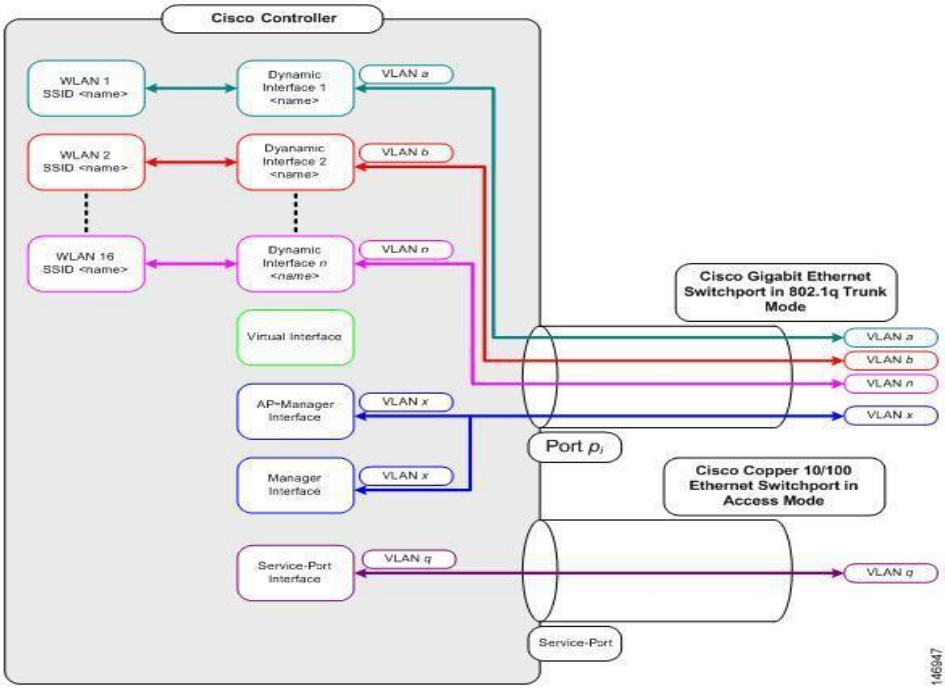

Рисунок 7.6 – Схематичний приклад VLAN, WLC

Під час налаштування на динамічному інтерфейсі контролера ви повинні використовувати теговані VLAN для динамічних інтерфейсів. Для налаштування динамічних інтерфейсів на контролері застосовуються такі обмеження: дротові клієнти не можуть отримати доступ до інтерфейсу керування Cisco 2504 WLC за допомогою IP-адреси інтерфейсу AP Manager. Для запитів SNMP, які надходять з підмережі, яка налаштована як динамічний інтерфейс, контролер реагує, але відповідь не потрапляє до пристрою, який ініціював підключення; якщо ви використовуєте проксі DHCP та / або вихідний інтерфейс RADIUS, переконайтеся, що динамічний інтерфейс має дійсну маршрутизацію.

Дубльовані або перекриваючі адреси через інтерфейси контролера не підтримуються; ви не повинні використовувати ім'я менеджера під час налаштування динамічних інтерфейсів asap-manageris зарезервованого імені.

Загальні відомості про LightWeight Access Point

Lightweight Access Point Protocol (LWAPP) — це протокол, розроблений Cisco для зв'язку між LightWeight Access Points (LAP) та Wireless LAN Controller (WLC), що дозволяє централізовано керувати точками доступу без необхідності їх локальної конфігурації. LWAPP спрощує розгортання бездротової мережі в великих організаціях, дозволяючи централізоване налаштування, моніторинг і оновлення для всіх точок доступу. Замість того, щоб кожна точка доступу мала свій окремий контроль, LWAPP забезпечує ефективну передачу даних між точками доступу та контролером, при цьому виконуючи більшість

обчислювальних і управлінських завдань на стороні контролера. Це дозволяє знизити навантаження на точки доступу, які більше не потребують складної обробки, а лише передають та отримують дані, що дозволяє краще масштабувати мережу.

LWAPP також включає механізми безпеки, що забезпечують шифрування даних, які передаються між точками доступу та контролером, що критично важливо для захисту бездротових мереж від атак та несанкціонованого доступу. Протокол також підтримує захист від відмов (redundancy) та дозволяє реалізувати міграцію клієнтів між точками доступу при русі, що забезпечує безперервну доступність бездротового з'єднання. Загалом LWAPP дозволяє адміністраторам зосередитися на управлінні мережею з єдиного пункту контролю, а також забезпечує високу ефективність і безпеку для великих і динамічних бездротових середовищ.

LWAPP був базовим протоколом побудови Уніфікованої Бездротової Мережі Cisco (Cisco Unified Wireless Network) включно до релізу 5.1, 2008 року.

До 2006 року, LWAPP - пропрієтарний протокол компанії Cisco, а згодом став робочим (draft) проєктом IETF. AES шифрування та режим лічильника з протоколом кодування автентифікації повідомлень з блокуванням шифрування блоків (CCMP) використовується для трафіку керування LWAPP.

CAPWAP (Control and Provisioning of Wireless Access Points) — це протокол, який замінив LWAPP як стандарт для централізованого управління точками доступу в бездротових мережах Cisco. CAPWAP забезпечує безпечний та ефективний спосіб зв'язку між Wireless LAN Controller (WLC) і Lightweight Access Points (LAP), дозволяючи централізовано налаштовувати, контролювати та моніторити точку доступу. Цей протокол використовує TLS (Transport Layer Security) для шифрування трафіку між точками доступу та контролером, що гарантує безпеку при передачі даних та захист від атак на мережу. CAPWAP підтримує кілька режимів передачі: управління (контролер з точки доступу), а також локальну обробку трафіку (наприклад, при використанні FlexConnect), що дозволяє покращити продуктивність та зменшити навантаження на контролер.

CAPWAP підтримує автоматичне виявлення контролера, що полегшує розгортання точок доступу у великих і складних мережах. Коли LAP підключається до мережі, він шукає контролер через Cisco Discovery Protocol (CDP) або DHCP Option 43 (який вказує IP-адресу контролера). Після встановлення з'єднання точка доступу і контролер здійснюють процес аутентифікації та обміну ключами для забезпечення безпеки з'єднання. Після успішного підключення контролер централізовано передає конфігурації LAP, включаючи параметри SSID, VLAN, політики безпеки тощо. Це дозволяє адміністратору з легкістю керувати великою кількістю точок доступу, що підключені до різних частин мережі, без необхідності ручного налаштування кожної точки доступу окремо. CAPWAP також підтримує функції мобільності, дозволяючи клієнтам безперешкодно переміщатися між різними точками доступу в межах однієї мережі. Схематична побудова зображена на рис. 7.7.

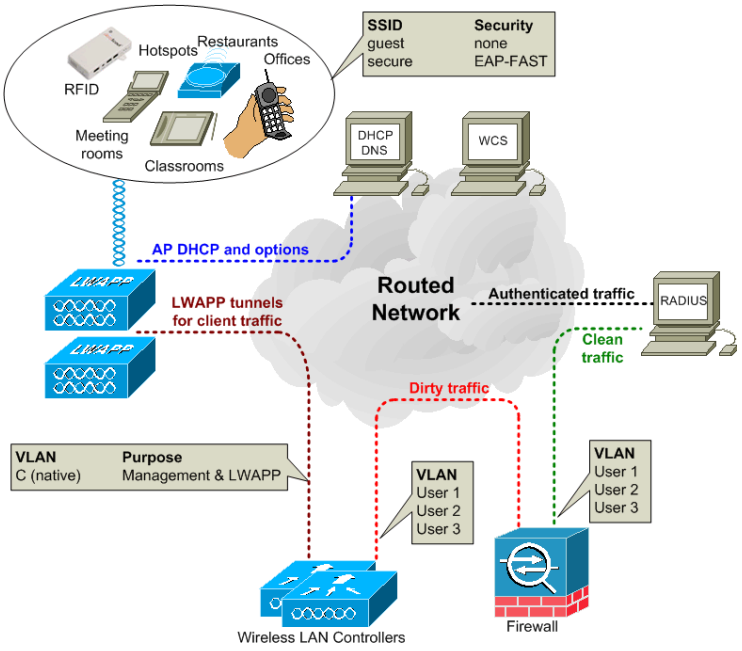

Рисунок 7.7 – Схематична побудова LightWeight Access Point

Операція LWAPP описується відповідно до топологічної схеми вище. Підключення Lightweight Access Point (LAP) до мережі через Wireless LAN Controller (WLC) включає кілька етапів, починаючи з фізичного підключення та закінчуючи налаштуванням через протокол LWAPP або CAPWAP (Cisco's proprietary protocol, що замінив LWAPP). Спочатку LAP підключається до мережі через Ethernet-кабель, при цьому може бути використаний Power over Ethernet (PoE) для живлення пристрою без необхідності в окремих джерелах живлення. Коли точка доступу підключена до мережі, вона автоматично намагається знайти WLC за допомогою Cisco Discovery Protocol (CDP) або DNS для отримання IP-адреси контролера. Якщо WLC не знайдений, точка доступу може використовувати DHCP для отримання IP-адреси та пошуку контролера за допомогою спеціально призначених DHCP-Option 43 або 60, що містять IP-адресу WLC.

Після того, як LAP знаходить WLC, відбувається встановлення з'єднання між ними через протокол LWAPP або CAPWAP. Спочатку точка доступу проходить процес аутифікації і заходить в режим "lightweight". Після цього WLC починає централізоване управління LAP: налаштовує SSID, політики безпеки, VLAN, та інші параметри мережі. LAP не зберігає локальні конфігурації, тому всі зміни, які виконуються на контролері, автоматично синхронізуються з точкою доступу. Це забезпечує централізоване адміністрування та легке масштабування мережі, оскільки для додавання нових точок доступу потрібно лише підключити їх до мережі, і вони автоматично отримають необхідну конфігурацію через контролер.

У режимі 3-го рівня AP надсилає запит на пошук LWAPP для IP-адреси менеджера AP за допомогою спрямованої трансляції. Якщо відповідь відсутня, AP надсилає широкомовний запит для будь-яких контролерів, які були знайдені з інших мереж через службу «По повітрю» (OTAP). Контролер реагує на

відповідь Discovery, який вказує кількість AP, пов'язаних з контролером. Потім AP надсилає до найменш завантаженого контролера запит на приєднання, який містить сертифікат AP.X.509.

Початкове підключення: Коли точка доступу підключається до мережі вперше, вона шукає Primary WLC через механізми як CDP або DHCP Option 43. Як тільки точка доступу знаходить контролер, вона з ним аутентифікується, і починається процес централізованого налаштування через LWAPP або CAPWAP, використовуючи сертифікати X.509. Це використовується для забезпечення процесу підключення та обміну контрольних пакетів даних LWAPP або CAPWAY. AP зареєстрований за допомогою WLC відповідно до параметрів апаратного забезпечення 60, які описують апаратний тип AP.

Резервування та автоматичне перемикання: Після успішного підключення, точка доступу також зберігає інформацію про Secondary WLC. Якщо Primary WLC не відповідає або стає недоступним, точка доступу автоматично спробує підключитися до Secondary WLC. Це забезпечує високу доступність мережі, оскільки клієнти і трафік можуть продовжувати працювати без серйозних перебоїв.

WLC оновлює програмне забезпечення AP, якщо це потрібно, і налаштовує AP за відповідними налаштуваннями бездротової мережі. Клієнтський пристрій намагається підключитись за SSID. Якщо потрібна автентифікація 802.1x, то облікові дані надсилаються через тунель LWAPP до WLC. WLC відображає SSID до відповідної VLAN користувача, і цей 802.1x трафік надходить у брандмауер.

Правила брандмауера дозволяють передати цей трафік на сервер RADIUS. Функція RADIUS може бути надана Cisco ACS (Access Control Server).

Сервер RADIUS перевіряє облікові дані та дозволяє користувачеві доступ до нього. Тепер користувацький пристрій отримує IP-адресу через DHCP через брандмауер. Корпоративна політика визначає, можливості користувача та його дозволи. Для ідентифікаторів SSID, які використовують WPA2-PSK для шифрування, на WLC встановлено різні мережеві ключі для кожного SSID. Користувачі повинні використовувати відповідний ключ, щоб отримати доступ до відповідної мережі. LWAPP використовує вихідний порт UDP 1024 і порт призначення 12222 для трафіку даних, порт UDP 1024 та порт 12223 UDP для керуючого трафіку.

Існує тенденція у просторі WLAN щодо централізованого інтелекту та контролю. У цій новій архітектурі - контролер WLAN система використовується для створення та забезпечення політики серед багатьох різних легких точок доступу. Централізоване керування надає безпеку, мобільність, якість обслуговування (QoS) та інші функції, необхідні для роботи з WLAN – по всій бездротовій мережі організації, також забезпечуючи розподіл функцій між контролером та точками доступу (рис. 7.8).

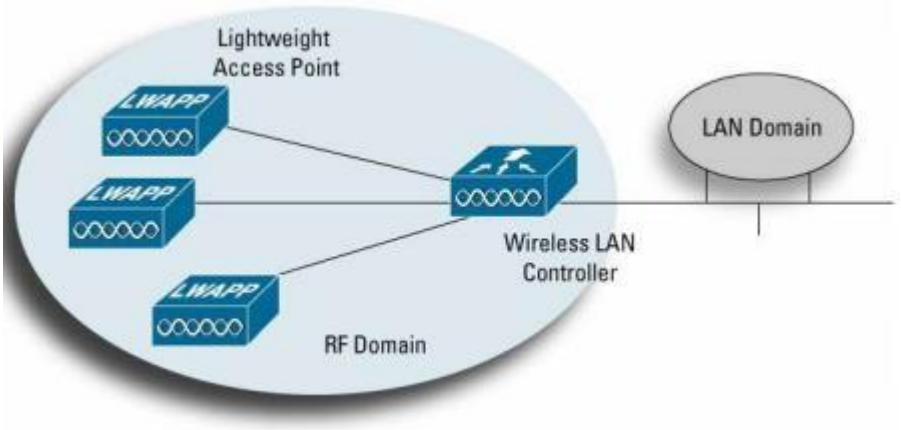

Рисунок 7.8 – WLAN системи централізованого інтелекту для широкого корпоративного управління підприємством та управління політикою

Традиційні рішення WLAN обмежують обробку трафіку, функції управління радіочастотним сигналом, безпеку та мобільність відносно до точки доступу. Зокрема, ця архітектура обмежує видимість трафіку 802.11 тільки для індивідуальної точки доступу (рис.4.9). Це означає:

- індивідуальні точки доступу, коли вони використовуються без керуючого пристрою, повинні бути налаштовані індивідуально, що може збільшити операційні витрати;
- єдина точка дотримання правил безпеки для Layer 1, Layer 2 та Layer 3;
- неможливо виявити та пом'якшити атаки відмови (DoS) у всій мережі WLAN;
- обмежена можливість увімкнення оптимізованого балансу навантаження в реальному часі;
- клієнти не можуть виконувати швидкі операції передачі даних, необхідні для підтримки додатків в режимі реального часу, таких як голос і відео.

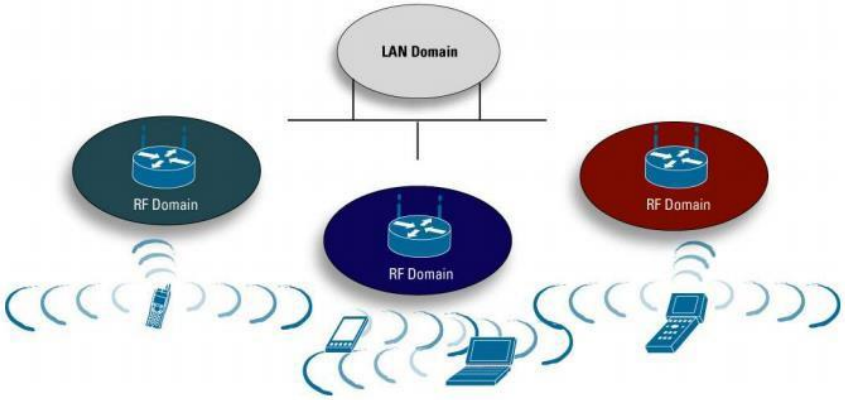

Рисунок 7.9 – Архітектура однорідної мережі WLAN обмежує продуктивність, керованість та безпеку

Оскільки з'являється більше продуктів, що використовують легкі точки доступу з централізованою інтелектуальною мережею WLAN, існує потреба у

галузевому стандарті, який керує тим, як ці пристрої спілкуються один з одним. LWAPP – це проєкт, який розглядається для стандартизації в роботі IETF. Керівник спочатку Airespace (придбаний компанією Cisco Systems у березні 2005 р.), та NTT DoCoMo, LWAPP стандартизує протокол зв'язку між точками доступу та системами WLAN (контролери, комутатори, маршрутизатори тощо). Мета цієї ініціативи, як описано нижче в специфікації IETF, полягає в тому, щоб:

- зменшити обсяг обробки в точці доступу, дозволяючи обмеженим обчислювальним ресурсам на цих пристроях зосередитися на бездротовій мережі доступ, на відміну від фільтрації та виконання політик;
- включити схему, за допомогою якої буде встановленя централізована обробка трафіку, автентифікація, шифрування та виконання політик (QoS, безпеки та ін.);
- забезпечити загальний механізм інкапсуляції та транспортування для взаємодії між точкою доступу та різноманітними джерелами через інфраструктуру рівня 2 або IP-маршрутизовану мережу.

Специфікація LWAPP працює для вирішення цих питань шляхом визначення наступних видів діяльності:

- відкриття точки доступу, обмін інформацією та конфігурація
- сертифікація точки доступу та контроль програмного забезпечення
- інкапсуляція пакунків, фрагментація та форматування
- управління та управління зв'язком між точкою доступу та бездротовим системним пристроєм.

Рекомендації стосовно підвищення рівня захищеності мереж, побудованих з використанням технологій VLAN

Багатьма виробниками обладнання розроблені базові рекомендації, що стосуються підвищення рівня захищеності комутованих мереж, які побудовані з використанням технологій VLAN. Часто ці рекомендації є комплексними і враховують використання і інших технологій та протоколів. Рекомендації щодо застосування VLAN, розроблені фірмою Cisco, є наступними:

1. Вимкнути усі незадіяні порти/інтерфейси комутатора та помістити їх у VLAN, що не використовується.
2. Використосувати як VLAN керування пристроєм нестандартну VLAN (будь-яку VLAN, окрім Default VLAN – VLAN 1, що створюється за замовчуванням).
3. Не використовувати VLAN 1 для будь-яких операцій та вимкнути його.
4. Налагодити всі порти/інтерфейси комутатора, до яких підключені кінцеві користувачі, як порти/інтерфейси доступу (вимкнути функціонування протоколу DTP на цих портах).
5. Точно (недвозначно) налагодити параметри транкових інфраструктурних портів/інтерфейсів.
6. Завжди використовувати призначені ідентифікатори (номери) VLAN для

всіх транкових портів/інтерфейсів.

7. Налагодити тегуваннння для Native VLAN на транкових каналах та налагодити відкидання нетегованих кадрів.

8. Встановити стан порта/інтерфеса за замовчуванням як вимкнений

Порядок налагодження VLAN на основі групування портів та транкових протоколів на комутаторі Cisco

Порядок налагодження віртуальної локальної мережі на базі комутатора Cisco при використанні групування портів та транкового протоколу 802.1Q згідно з рекомендаціями виробника є таким:

1. Створити віртуальну локальну комп’ютерну мережу (обов'язково).
2. Вказати назву для створеної віртуальної локальної комп’ютерної мережі (необов'язково).
3. Для обраного інтерфейсу/порту доступу (або групи інтерфейсів/портів) вказати тип – інтерфейс/порт доступу (необов'язково).
4. Для обраного інтерфейсу/порту доступу (або групи інтерфейсів/портів) вказати належність до створеної віртуальної локальної комп’ютерної мережі (обов'язково).
5. Для обраного транкового інтерфейсу/порту (або групи інтерфейсів/портів) вказати тип – транковий інтерфейс/порт (обов'язково).
6. Для обраного транкового інтерфейсу/порту налагодити додаткові параметри транкового каналу (необов'язково).
7. Для обраного транкового інтерфейсу/порту налагодити додаткові параметри передачі кадрів (заборонені і дозволені VLAN, native VLAN тощо) (необов'язково).

Команди налагодження VLAN на основі групування портів та транкових протоколів на комутаторах Cisco

Якщо виникає потреба налагодити транковий канал без використання протоколу DTP (наприклад, якщо один із пристроїв, що входять до складу каналу не є пристроєм Cisco), у парі з командою **switchport mode trunk** застосовується команда **switchport nonegotiate**. Результатом роботи цих команд є те, що канал активується, а повідомлення протоколу DTP не пересилаються. Команда **switchport trunk** дає змогу здійснювати специфічне налагодження транкового каналу, наприклад, дозволити передачу кадрів одних VLAN і заборонити передачу кадрів інших.

Команда **switchport priority** дає змогу встановлювати пріоритети для кадрів, що належать різним VLAN.

Команда **switchport native vlan** застосовується для встановлення певної **VLAN**, як **Native VLAN** – **VLAN**, кадри якої не тегуються при передачі через транковий канал. Відміна дії вищезгаданих команд – використання форми **no**. Синтаксис розглянутих команд та режими їх застосування наведено нижче.

Синтаксис команди vlan (режим глобального конфігурування): **vlan vlan-id**, де **vlan-id** – ідентифікатор (номер) VLAN, може зазначатися в межах від 1 до 4094, для мереж Ethernet типове використання у діапазоні від 2 до 1001. Синтаксис команди name (режим конфігурування VLAN):

name text-string, де **text-string** – текстова назва **VLAN**; якщо текстова назва **VLAN** явно не зазначається, то система автоматично встановлює назву вигляду **VLANDDDD**, де DDDD – чотирицифровий десятковий номер **VLAN**.

Синтаксис команди **switchport access vlan** (режим конфігурування інтерфейсу/групи інтерфейсів):

switchport access vlan {vlan-id | dynamic}, де **vlan-id** – ідентифікатор VLAN; **dynamic** – параметр, який зазначає, що належність інтерфейсу/порту до **VLAN** визначається динамічно (за MAC- адресою), шляхом запиту до сервера **VMPS (VLAN Membership Policy Server)**.

Синтаксис команди **switchport host** (режим конфігурування інтерфейсу/групи інтерфейсів): **switchport host** – команда не має параметрів.

Синтаксис команди **switchport mode** (режим конфігурування інтерфейсу/групи інтерфейсів):

switchport mode {access | dynamic {auto | desirable} | trunk}, де **access** – зазначає тип інтерфейсу/порту – інтерфейс/порт доступу; **trunk** – зазначає тип інтерфейсу/порту – транковий інтерфейс/порт та активує стан trunk (відповідає значенню on);

dynamic – встановлення переговорного режиму для транкового інтерфейсу, може доповнюватися значенням **auto** або **desirable**; за замовчуванням встановлюється **dynamic auto**;

auto – інтерфейс/порт знаходиться в автоматичному режимі і буде переведений у стан trunk, як тільки інтерфейс на іншому кінці знаходиться у режимі **on** або **desirable**;

desirable – інтерфейс/порт готовий перейти у стан trunk залежно від стану інтерфейсу на іншому кінці каналу.

Синтаксис команди **switchport nonegotiate** (режим конфігурування інтерфейсу/групи інтерфейсів):

switchport nonegotiate – команда не має параметрів.

Синтаксис команди **switchport trunk** (режим конфігурування інтерфейсу/групи інтерфейсів):

switchport trunk {allowed vlan vlan-list | native vlan vlan-id | pruning vlan vlan-list}, де **allowed vlan** – службова конструкція, за допомогою якої створюється список дозволених VLAN, для яких транковий інтерфейс може пересилати та отримувати трафік у тегованій формі; за замовчуванням **vlan-list** для цієї конструкції дорівнює **all**; **vlan-list** у цьому випадку не може дорівнювати

none;

native vlan – службова конструкція, за допомогою якої створюється список VLAN, для яких транковий інтерфейс може пересилати і отримувати трафік у нетегованій формі;

Синтаксис команди **interface** (режим глобального конфігурування):

interface interface-type interface-id.subinterface-id, де:

interface-type – тип інтерфейсу (порту), може набувати значень Ethernet, FastEthernet, GigabitEthernet, Port-channel;

interface-id – ідентифікатор інтерфейсу (порту), може мати одночислове позначення **number** (номер порту), або двочислове позначення **module/number** (номер модуля/номер порту);

subinterface-id – ідентифікатор під інтерфейсу (порту), число у десятковій формі з діапазону 0– 4294967295. Створювати логічний під інтерфейс можна за допомогою команди **interface** як у режимі глобального конфігурування, так і у режимі конфігурування інтерфейсу Ethernet.

Синтаксис команди **encapsulation dot1q** (режим конфігурування під інтерфейсу Ethernet):

encapsulation dot1q vlan-id [native | second-dot1q {vlan-list | any}, де **dot1q** – службова конструкція, за допомогою якої вказується, що виконується інкапсуляція згідно зі стандартом 802.1q; **vlan-id** – ідентифікатор (номер) VLAN, може зазначатися у межах від 1 до 4094, для мереж Ethernet характерне використання у діапазоні від 2 до 1001;

native – параметр, який вказує, що поточну VLAN використовувати як VLAN типу native;

second-dot1q – параметр, який вказує, що поточний інтерфейс налаштовується для підтримки стандарту **Q-in-Q**;

vlan-list – список внутрішніх VLAN вигляду 100-200,422,500-550; **any** – параметр, який вказує всі внутрішні VLAN, що не налагоджені на інших під інтерфейсах.

Таблиця 1

Перелік команд *show* діагностики роботи VLAN на комутаторах Cisco

Команда	Призначення
show vlan	Виведення всієї інформацію про VLAN та їх параметри
show vlan brief	Виведення інформації про VLAN у скороченому вигляді
show vlan id *vlan-id*	Виведення інформаціїпроVLAN за її ідентифікатором(номером)
show vlan name *vlan-name*	Вивести інформацію про VLAN за її назвою
show vlan summary	Виведення сумарної інформації про кількість створених VLAN, кількість VLAN із розширеного діапазону, кількікість VTP VLAN.
show interfaces switchport	Виведення інформації про налагодження параметрів VLAN для всіх інтерфейсів/портів
show interfaces *interface-type interface-id* switchport	Виведення інформації про налагодження параметрів VLAN для певного інтерфейсу/порту

Закінчення табл. 1

show interfaces trunk	Виведення інформації про транкові канали та їх параметри
show interfaces vlan ***vlan-id***	Виведення інформації про параметри інтерфейсу певної VLAN. Інтерфейс повинен бути попередньо створений
show dtp	Виведення інформації про параметри інформаційного обміну за протоколом DTP для комутатора
show dtp interface ***interface-type interface-id***	Виведення інформації про параметри інформаційного обміну за протоколом DTP для певного транкового інтерфейсу

Команди функціонування LightWeight Access Point

Налагодження функціонування контролера LightWeight Access Point може здійснюватися як на маршрутизаторах, так і на комутаторах 3-го рівня, виготовлених фірмою Cisco. Деякі відмінності у процесі налагодження можуть виникати через особливості синтаксису команд та версій Cisco IOS. Слід пам’ятати, що налагодження виконується не на маршрутизаторі в цілому, а лише на певному його інтерфейсі. Одні з команд для перевірки та налаштування LightWeight Access Point:

capwap ap hostname – налаштування назви вузла точки доступу з порту консолі точки доступ;

capwap ap ip default-gateway – налаштування шлюзу за замовчуванням з консольного порту точки доступу;

capwap ap log-server – налаштування системного журналу для реєстрації всіх помилок CAPWAP4;

capwap ap primary-base – налаштування ім'я основного контролера та IP-адреси в точку доступу CAPWAP з доступом консольного порта точки;

capwap ap primed-timer {enable | disable} – налаштування закріпленого таймера у точці доступу CAPWAP;

capwap ap tertiary-base – налаштування назви та IP-адреси третього рівня Cisco WLC у точках доступу CAPWAP з консольним портом точки доступу;

config {802.11-a49 | 802.11-a58} antenna extAntGain – налаштуваня посилення зовнішньої антени для каналів громадської безпеки 4,9 ГГц та 5,8 ГГц на доступ точки:

802.11-a49 – визначає канал громадського безпеки 4,9 ГГц;

802.11-a58 – визначає канал громадського безпеки 5,8 ГГц;

ant_gain – значення в одиницях .5-dBi (наприклад, 2,5 дБі = 5);

cisco_ap – назва точки доступу, до якої застосовується команда;

global – вказує значення посилення антени для всіх каналів;

channel_no – антена отримує значення для певного каналу.

config 802.11-a txpower ap – налаштування власних властивостей передачі для каналів громадської безпеки 4,9 ГГц і 5,8 ГГц на точки доступа***;***

config advanced 802.11{a | b} profile utilization {global | cisco_ap} percent – щоб встановити поріг використання радіочастот від 0 до 100 відсотків, використовуйте розширений профіль 802.11 config – команда використання. Операційна система генерує пастку при перевищенні цього порога:

a – визначає мережу 802.11a;

b – визначає мережу 802.11b / g;

global – налаштовує глобальний профіль Cisco для легкого доступу до точки доступу;

cisco_ap – найменування назви точки доступу Cisco;

percent – 802.11a рівень використання RF у межах від 0 до 100 відсотків.

config ap autoconvert – для автоматичного перетворення всіх точок доступа в режим FlexConnect або в режимі монітора, зв'язавшись з Cisco WLC.

flexconnect – налаштовує всі точки доступу автоматично у режим FlexConnect;

monitor – автоматично налаштовує всі точки доступу до режиму моніторингу;

disable – вимкнено параметр автоматичного перетворення в точках доступу.

config ap static-ip – налаштувати параметри статичної IP-адреси в точці доступу Cisco:

disable – відключити Cisco Lightweight точки доступу статичної IP-адреси. Точки доступу використовують DHCP отриману IP-адресу.

domain – визначає домен, до якого певна точка доступу або всі точки доступу належать.

Модельний приклад налагодження Cisco WLC 2504

Розглянемо специфіку налагодження роботи Wireless Lan Controller, схема якої зображена на рис. 7.10.

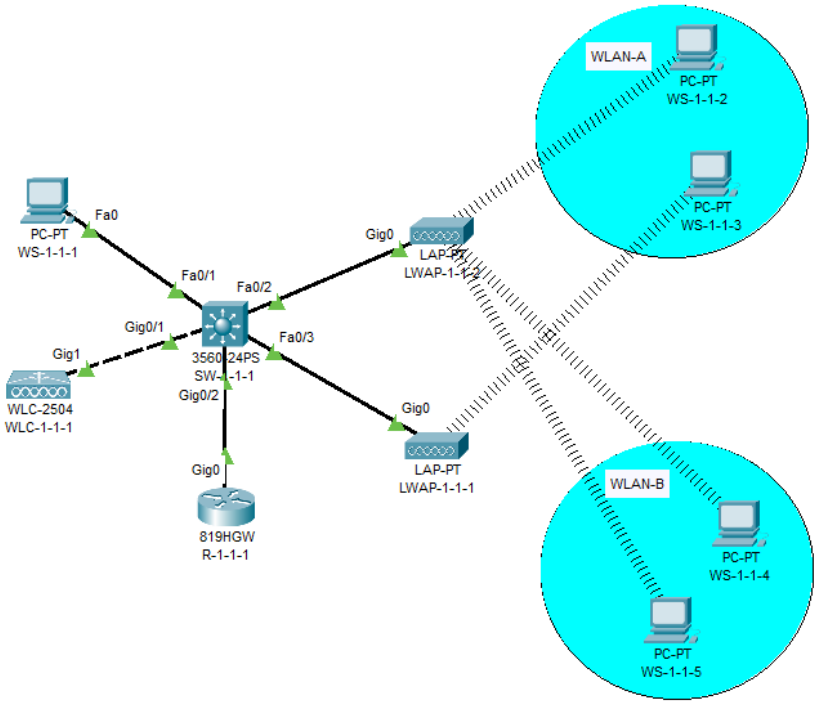

Рисунок 7.10 – Приклад топології мережі з Cisco WLC 2504

Під час побудови даної мережі для з'єднання пристроїв використано дані табл. 3. Для налагодження параметрів адресації пристроїв використано дані табл. 3.

Таблиця 2

Параметри інтерфейсів пристроїв для прикладу 2504

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Wireless Lan Controller	Gig1	L3-комутатор	Fa0/2
	Gig0/1		Fa0/3
			Gig0/1
L3-комутатор	Fa0/2	Wireless_0	Gig0
	Fa0/3	Wireless_1	Gig0
	Fa0/1	WS-1-1-1	Fa0
Робоча станція WS-1-1-2	Wireless_0	LWAP-1-1-2	Fa0/2
Робоча станція WS-1-1-4	Wireless_1	LWAP-1-1-1	Fa0/3

Таблиця 3

Параметри адресації мережі WLC 2504

	WLC	Admin	Vlan
IP	192.168.1.3	192.168.1.4	192.168.1.1
Mask	255.255.255.0	255.255.255.0	255.255.255.0
Default gateway	192.168.1.1	192.168.1.1	—
DNS	—	192.168.1.3	—

Розглянемо порядок первинного налаштування маршрутизатора для роботи в мережі для однієї підмережі адміністрування:

```
Router>enable
Router# configure terminal
Router(config)# interface GigabitEhternet 0/0.80
Router(config)# encapsulation dot1Q 80
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
```

Підінтерфейси користувачів налаштовуються аналогічним чином:

Router>enable
Router# configure terminal
Router(config)# interface GigabitEhternet 0/0.190
Router(config)# encapsulation dot1Q 190
Router(config-if)# ip address 190.1.1.1 255.255.255.224
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface GigabitEhternet 0/0.191
Router(config)# encapsulation dot1Q 191
Router(config-if)# ip address 191.1.1.1 255.255.255.128
Router(config-if)# no shutdown
Router(config-if)# exit

Первинне налаштування багаторівневого комутатора Cisco Switch 3560:

Switch>enable
Switch# configure terminal
Switch(config)# interface vlan <VLAN ID адміністрування>
Switch(config-if)# ip address 192.168.1.2 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface vlan <VLAN ID клієнтів A>
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface vlan <VLAN ID клієнтів B>
Switch(config-if)# no shutdown
Switch(config-if)# exit

Switch(config)# interface FastEthernet 0/1
Switch(config-if)# description LINK-to-PCAdmin
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan <VLAN ID адміністрування>

Switch(config)# interface FastEthernet 0/2
Switch(config-if)# description LINK-to-WLC
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan <VLAN ID адміністрування>

Switch(config)# interface FastEthernet 0/3
Switch(config-if)# description LINK-to-LWAP1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport trunk native vlan <VLAN ID адмін.>
Switch(config-if)# switchport mode trunk

Switch(config)# interface FastEthernet 0/4
Switch(config-if)# description LINK-to-LWAP2
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport trunk native vlan <VLAN ID адмін.>
Switch(config-if)# switchport mode trunk
Switch(config)# interface FastEthernet 0/5
Switch(config-if)# description LINK-to-Router
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit

Подальше налаштування пристроїв мережі можна виконати за двома сценаріями:

1) Створення та налаштування усіх необхідних DHCP-серверів відбувається на маршрутизаторі;
2) На маршрутизаторі налаштовуються **тільки** DHCP-сервери для клієнтів, тоді як DHCP-сервер підмережі адміністрування буде налаштовано на багаторівневому комутаторі Cisco Switch 3560.

Налаштування пристроїв за кожним із запропонованих сценаріїв наведено нижче.

Сценарій 1. Налагодження усіх DHCP-серверів на маршрутизаторі

Router(config)# ip dhcp pool internal
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# dns-server <IP-адреса WLC>
Router(dhcp-config)# exit
Router(config)# ip dhcp excluded-address 192.168.1.1
Router(config)# ip dhcp excluded-address 192.168.1.2
Router(config)# ip dhcp excluded-address 192.168.1.3
Router(config)# ip dhcp excluded-address 192.168.1.4
Router(config)# service dhcp

Router(config)# ip dhcp pool WLAN-A
Router(dhcp-config)# network 190.1.1.0 255.255.255.224
Router(dhcp-config)# default-router 190.1.1.1
Router(dhcp-config)# dns-server 190.1.1.1
Router(dhcp-config)# exit
Router(config)# ip dhcp excluded-address 190.1.1.1
Router(config)# ip dhcp excluded-address 190.1.1.2

Router(config)# ip dhcp pool WLAN-B
Router(dhcp-config)# network 191.1.1.0 255.255.255.128
Router(dhcp-config)# default-router 191.1.1.1
Router(dhcp-config)# dns-server 191.1.1.1

Router(dhcp-config)# exit
Router(config)# ip dhcp excluded-address 191.1.1.1
Router(config)# ip dhcp excluded-address 191.1.1.2

Сценарій 2. Налагодження DHCP-сервера підмережі адміністрування на багаторівневому комутаторі Cisco Switch 3560

Switch(config)# ip dhcp pool internal
Switch(dhcp-config)# network 192.168.1.0 255.255.255.0
Switch(dhcp-config)# default-router 192.168.1.1
Switch(dhcp-config)# dns-server <IP-адреса WLC>
Switch(dhcp-config)# exit
Switch(config)# ip dhcp excluded-address 192.168.1.1
Switch(config)# ip dhcp excluded-address 192.168.1.2
Switch(config)# ip dhcp excluded-address 192.168.1.3
Switch(config)# ip dhcp excluded-address 192.168.1.4
Switch(config)# service dhcp

Подальші налаштування DHCP-серверів для клієнтів підмереж A та B виконуються на маршрутизаторі, аналогічно сценарію 1.

Налаштування Cisco WLC 2504

Підключіться до WLC 2504, використовуючи веб-браузер робочої станції адміністрування, задаючи адресу: http://<IP-адреса WLC> − налаштуйте ім'я користувача та пароль адміністратора. Адміністративними повноваженнями буде логін: admin, пароль: P@ssw0rd в цьому посібнику. Переконайтеся, що для цього першого з'єднання використовується протокол HTTP (незахищений), а не HTTPS (рис. 7.11).

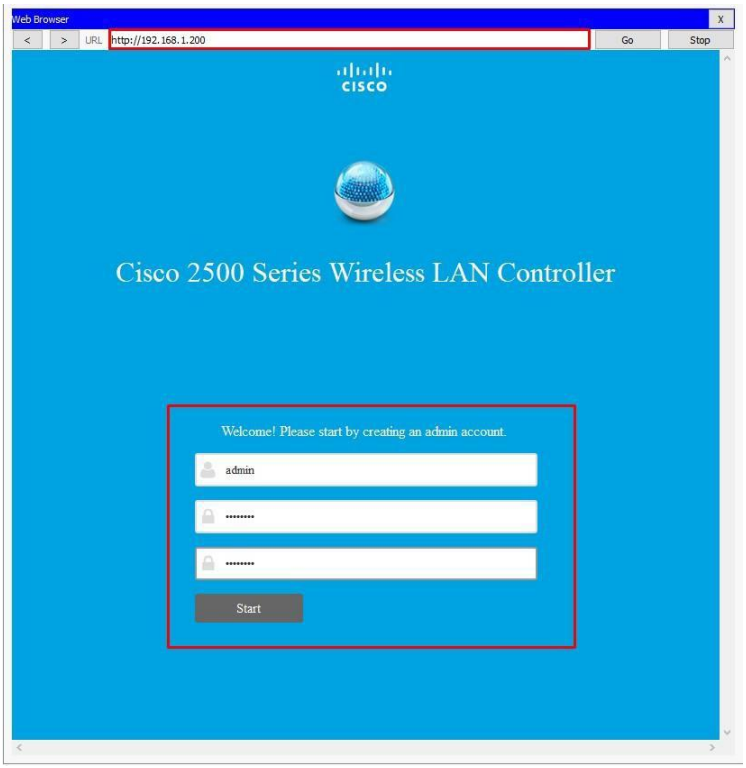

Рисунок 7.11 – Створення нового користувача-адміністратора

Необхідно виконати початкові налаштування WLC, задати системне ім'я, дату та час (задаються автоматично, але за потреби їх можна змінити), IP-адресу керування (вкажіть адресу, яка призначена інтерфейсу management даної WLC), та шлюз за замовчуванням (вкажіть IP-адресу інтерфейса VLAN керування, або IP-адреса маршрутизатора, наприклад 192.168.1.1) (рис. 7.12). У полі **<Management VLAN ID>** вкажіть «**1**» Після цього натисніть «Next», де Ви можете подивитись задані налаштування перед збереженням, як показано на рис. 7.13. Переконайтесь що все вказано вірно, після чого можете натискати «Next» ще раз. Відкриється вікно підтвердження Ваших налашувань та попередження що WLC буде перезавантажений, як показано на рис. 7.14. Натискайте «OK», після чого можете закривати бразузер. **Не чекайте завантаження сторінки. Необхідно прискорити час симуляції мережі, так як процес перезавантаження WLC займає багато часу**.

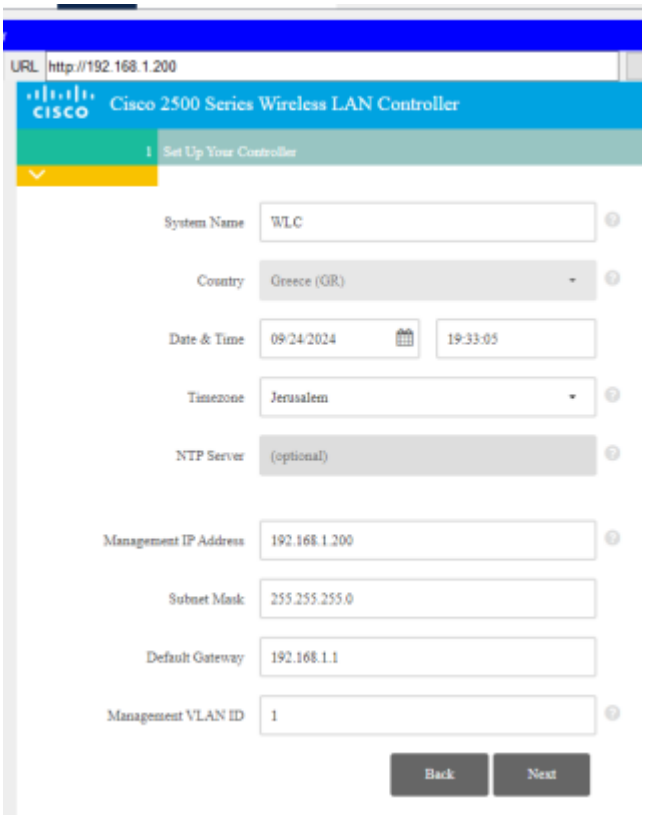

Рисунок 7.12 – Налаштування WLC

Рисунок 7.13 – Завершальний процес застосування

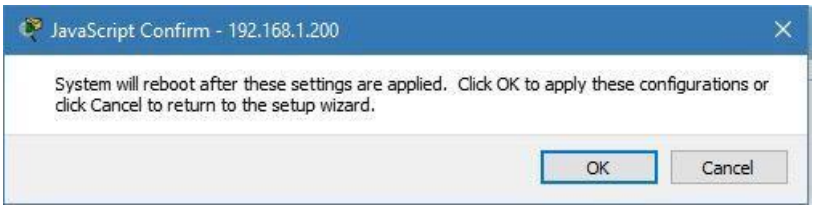

Рисунок 7.14 – Підтвердження перезавантаження WLC

Після завершення початкового процесу налаштування, підключіться повторно до Cisco WLC за допомогою **HTTPS** (https://<IP-адреса WLC>) (рис. 7.15) . Якщо ви намагаєтесь підключитись за допомогою HTTP (незахищений), WLC відкидатиме підключення. Далі, натисніть «Login» для відкриття вікна, де ви повинні ввести свої облікові дані, які були задані на попередньому етапі.

Рисунок 7.15 – Вікно входу до WLC після початкового налаштування

Легкі точки доступу автоматично виявляють адресу WLC, використовуючи опцію DHCP 150, налаштовану на DHCP, яка була налаштована на перемикач Catalyst для Vlan 1 (рис. 7.16).

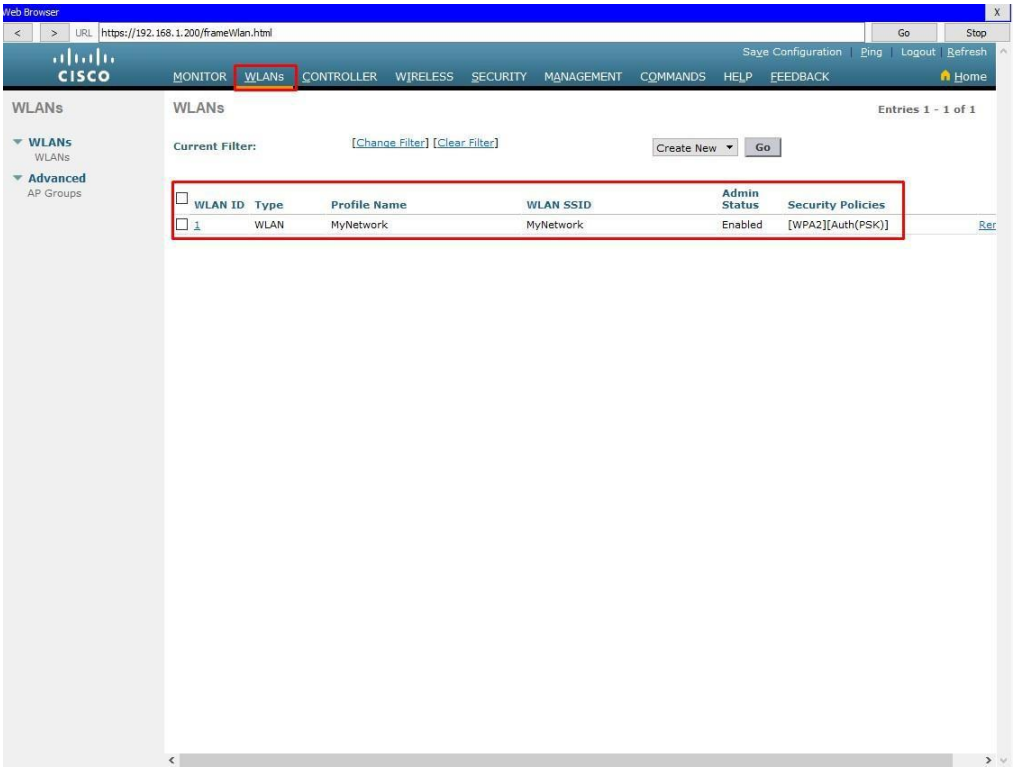

Рисунок 7.16 – Створення WLAN

WLC відображає успішно зареєстровані точки доступу з цією IP-адресою. докладні дані недоступні, оскільки ця функція не була реалізована в Packet Tracer. Приклад зображений на рис. 7.17.

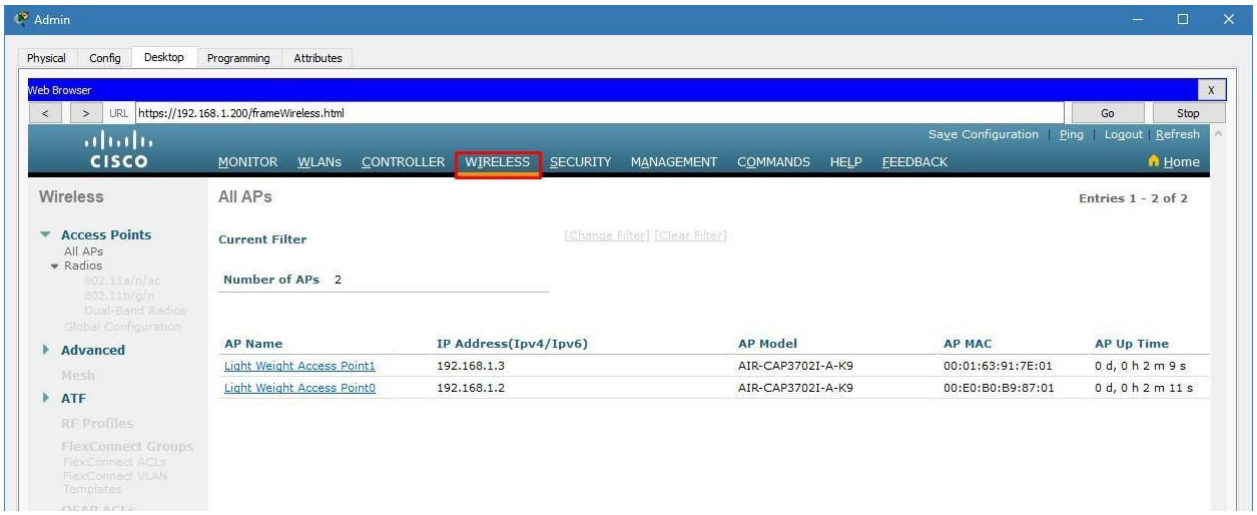

Рисунок 7.17 – Успішно зареєстровані точки доступу

Створення інтерфейсів WLAN на WLC

Перейдіть на вкладку «**Controller**» і далі оберіть пункт меню зліва: «**Interfaces**». Натисніть на кнопку «**New…**» у правому верхньому кутку, після чого має завантажитись сторінка створення нового інтерфейсу. Необхідно вказати назву інтерфейсу, та VLAN ID підмережі клієнтів (рис. 7.18.1-2). Якщо все вказали правильно, тоді можна натиснути кнопку «Apply».

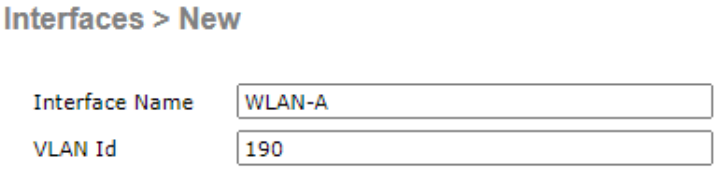

Рисунок 7.18.1 – Створення нового WLAN інтерфейсу на WLC

Далі натисніть на ID WLAN інтерфейсу (якщо налаштування не відкрились автоматично) і вкажіть додаткові параметри:

- Port Number – WLC підключена до комутатора через GigabitEthernet1, тому вказуємо «1»;
- VLAN Identifier – ідентифікатор VLAN підмережі клієнтів, у прикладі це - 190.1.1.0, де номер VLAN також «190» тому вказуємо саме його;
- IP Address – IP-адреса цього WLAN інтерфейсу у підмережі користувачів;
- Gateway – шлюз за замовчуванням, зазвичай це IP-адреса маршрутизатора.

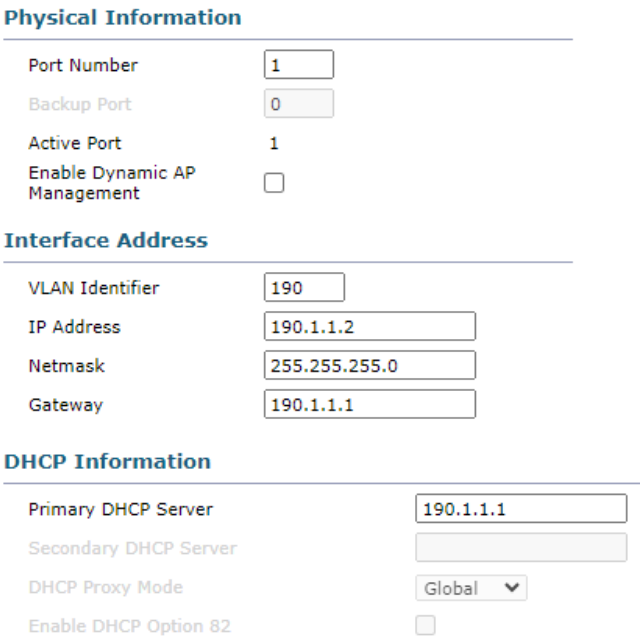

Рисунок 7.18.2 – Приклад налаштування WLAN інтерфейсу

Створення WLAN на WLC

Перейдіть до вкладки «WLANs», а далі натисніть на кнопку «Go» для того щоб створити нову WLAN (рис. 7.19).

Рисунок 7.19 – Створення нової WLAN

Задайте назву профілю та SSID який буде транслюватись для клієнтів (рис. 7.20).

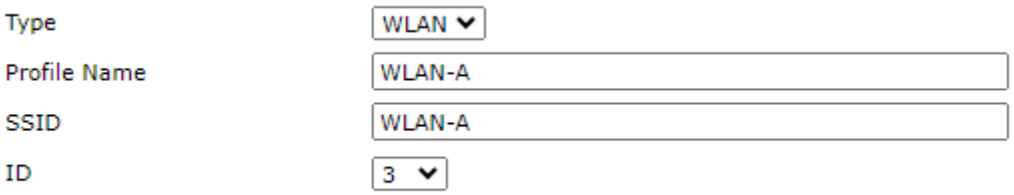

Рисунок 7.20 – Параметри створення нової WLAN

Після успішного створення WLAN необхідно налаштувати метод автентифікації та обрати відповідний інтерфейс замість «management» (рис. 7.21).

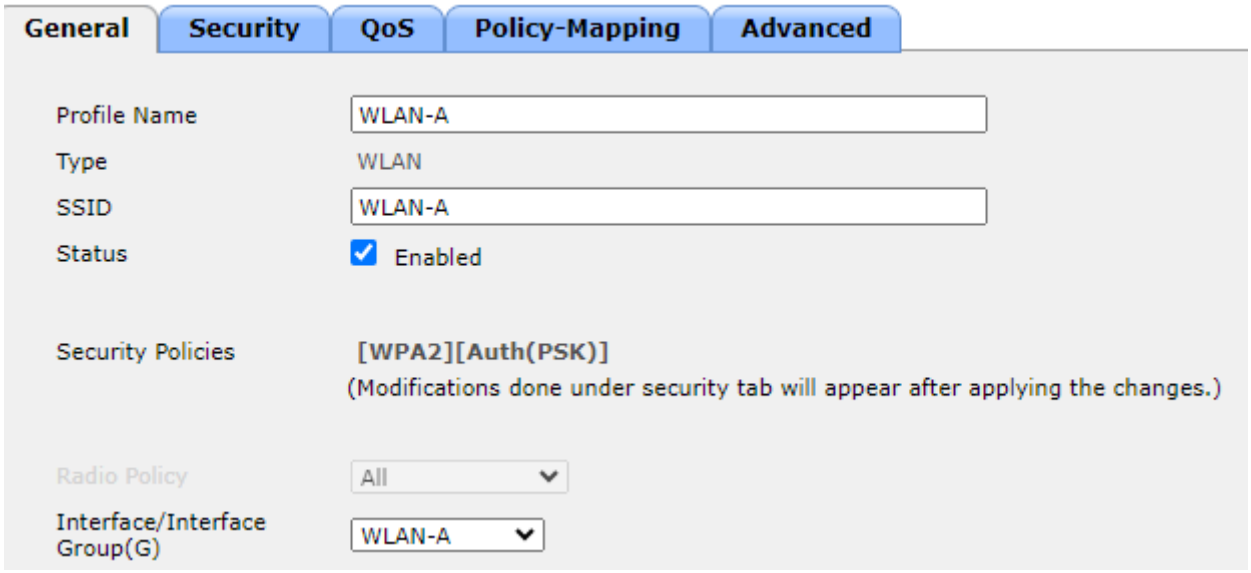

Рисунок 7.21 – Налаштування WLAN

Важливо! Після створення та налагодження кожної WLAN, також необхідно увімкнути функцію “FlexConnect”, інакше WLAN не буде транслюватись. Для цього треба перейти до вкладки «WLAN’s», обрати потрібний WLAN, перейти до меню «Advanced» та увімкнути два параметри “FlexConnect”, як зображено на рис. 7.22.

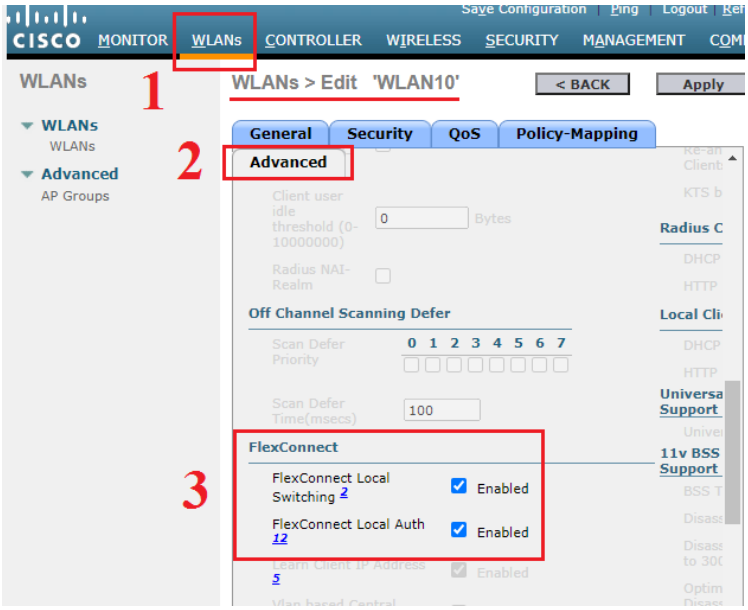

Рисунок 7.22 – Налаштування FlexConnect для WLAN

Для розподіленого підключення робочих станцій до точок доступу, варто зменшити радіус їхньої дії до 50 м, як показано на рис. 7.23.

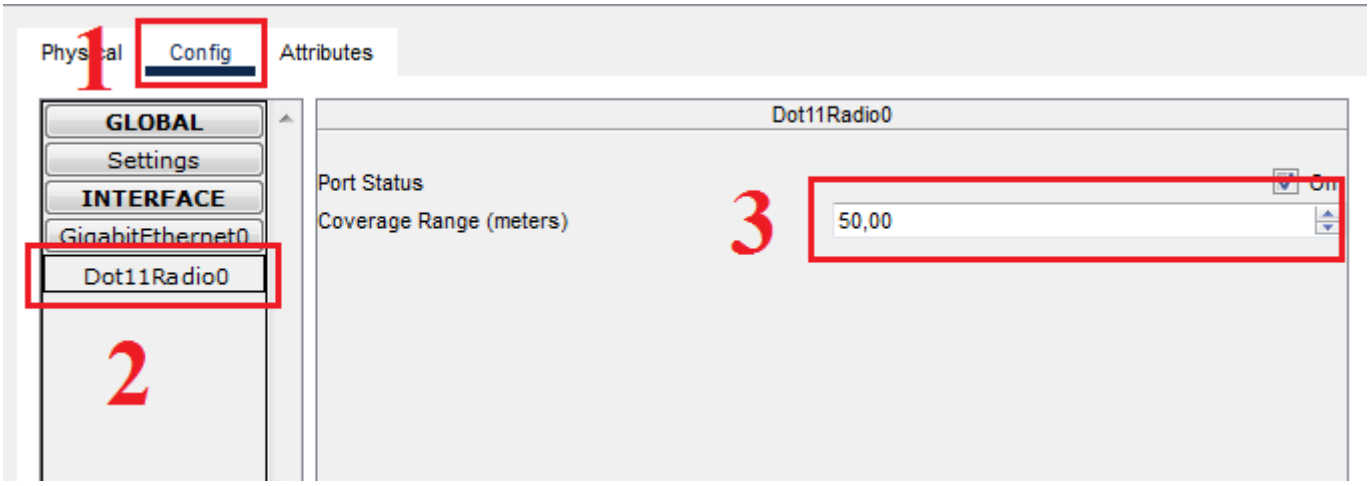

Рисунок 7.23 – Налаштування радіусу дії точки доступу

Завдання на лабораторну роботу

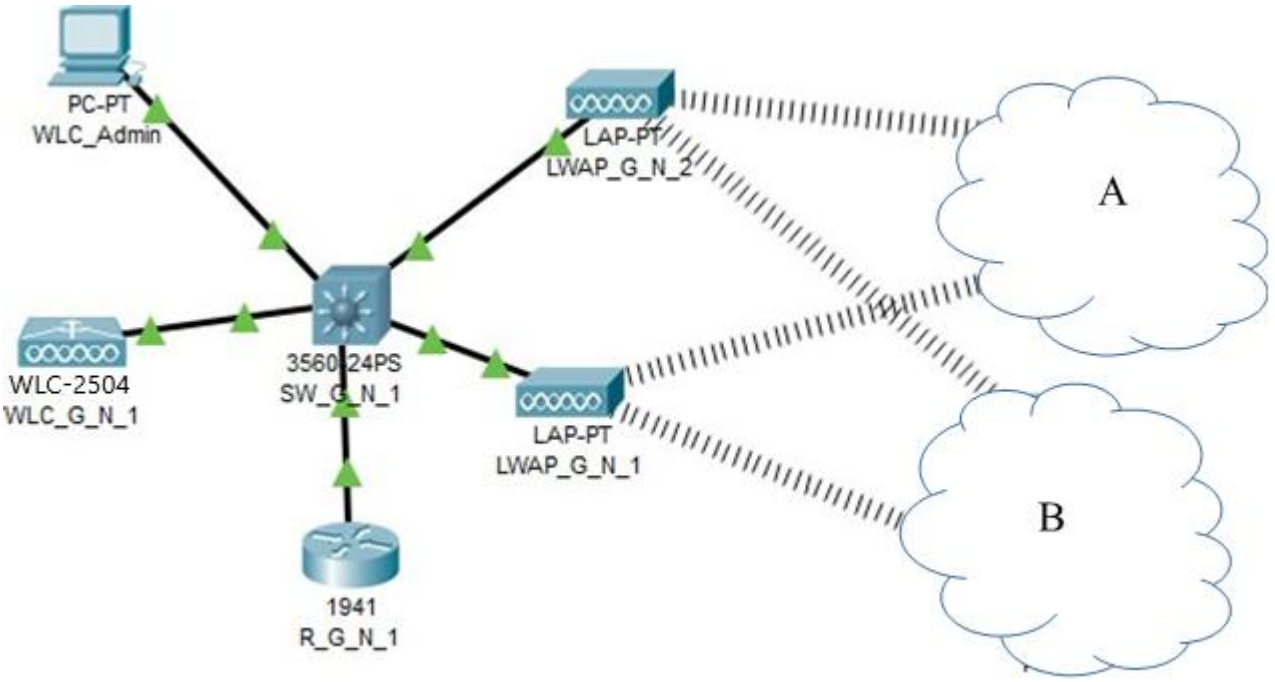

Рисунок 7.24 – Топологія мережі Wireless Lan Controller

1. У середовищі програмного симулятора/емулятора створити проєкт мережі (рис. 7.20). Під час побудови мережі звернути увагу на вибір моделей мережевих пристроїв, мережевих модулів та адаптерів, а також мережевих з'єднань. Задіяне обладнання та використані інтерфейси для побудованої мережі, записати до описової таблиці, яка аналогічна табл. 2.
2. Розробити схему адресації пристроїв мережі. Для цього скористатися даними табл. 4. Результати навести у вигляді таблиці, яка аналогічна табл. 3. Номер мережі адміністрування обираєте довільний.
3. У побудованій мережі налагодити функціонування WLC на основі групування портів, використати маршрутизатор, налагодити автентифікацію користувачів до WLAN та створити VLAN керування за параметрами, зазначеними у табл. 5. Номери та назви VLAN для користувачів обрати згідно першого байту адреси мережі. Виконати додаткові налагодження, які забезпечать підвищення рівня захищеності побудованої мережі.
4. Налагодити LightWeight Access Point, а також DHCP-сервер на R_G_N_1**.**
5. Дослідити особливості та отримання службової та діагностичної інформації про налагоджені WLC, перевірити наявність зв'язку між робочими станціями WLAN та іншими пристроями мережі.

Таблиця 4

Дані для адресації підмереж (каналів)

№ варіанта	Підмережа А		Підмережа В	
	IP-адреса	Префікс	IP-адреса	Префікс
1	193.G.N.0	/27	194.G.N.0	/24
2	193.G.N.64	/27	194.G.N.0	/24
3	193.G.N.128	/27	194.G.N.0	/25
4	193.G.N.192	/27	194.G.N.0	/25
5	193.G.N.0	/28	194.G.N.0	/25
6	193.G.N.32	/28	194.G.N.0	/24
7	193.G.N.64	/28	194.G.N.0	/25
8	193.G.N.96	/28	194.G.N.0	/24
9	193.G.N.128	/28	194.G.N.0	/25
10	193.G.N.160	/28	194.G.N.0	/24
11	193.G.N.192	/28	194.G.N.0	/25
12	193.G.N.224	/28	194.G.N.0	/24
13	193.G.N.0	/25	194.G.N.0	/25
14	193.G.N.0	/26	194.G.N.0	/25
15	193.G.N.128	/26	194.G.N.0	/24
16	193.G.N.0	/27	194.G.N.0	/25
17	193.G.N.64	/27	194.G.N.0	/24
18	193.G.N.128	/27	194.G.N.0	/25
19	193.G.N.192	/27	194.G.N.0	/24
20	193.G.N.0	/26	194.G.N.0	/24
21	193.G.N.32	/28	194.G.N.0	/25
22	193.G.N.64	/28	194.G.N.0	/25
23	193.G.N.96	/28	194.G.N.0	/24
24	193.G.N.128	/28	194.G.N.0	/24
25	193.G.N.160	/28	194.G.N.0	/25

Таблиця 5

Параметри налагодження

№ варіанту	Маршрутизатор R_G_N_2	Автентифікація клієнтів до WLAN	ID VLAN керування
1	819	WEP	91
2	829	WPA2-PSK	92
3	2911	Open	93
4	819	WPA2-PSK	94
5	829	Open	95
6	2911	WEP	96
7	819	Open	97
8	829	WEP	98
9	2911	WPA2-PSK	99
10	819	WEP	100
11	829	WPA2-PSK	101
12	2911	Open	102
13	819	WPA2-PSK	103
14	829	Open	104
15	2911	WEP	105
16	819	Open	106
17	829	WEP	107
18	2911	WPA2-PSK	108
19	819	WEP	109
20	829	WPA2-PSK	110
21	2911	Open	111
22	819	WPA2-PSK	112
23	829	Open	113
24	2911	WEP	114
25	819	Open	115

Таблиця 6

Клієнти

№ варіанту	Підмережа A	Підмережа B
1	DHCP	DHCP
2	DHCP	Static
3	Static	DHCP
4	DHCP	DHCP
5	DHCP	Static
6	Static	DHCP
7	DHCP	DHCP
8	DHCP	Static
9	Static	DHCP
10	DHCP	DHCP
11	DHCP	Static
12	Static	DHCP
13	DHCP	DHCP
14	DHCP	Static
15	Static	DHCP
16	DHCP	DHCP
17	DHCP	Static
18	Static	DHCP
19	DHCP	DHCP
20	DHCP	Static
21	Static	DHCP
22	DHCP	DHCP
23	DHCP	Static
24	Static	DHCP
25	DHCP	DHCP

Контрольні питання

1. Як розшифровується абревіатура WLC?
2. Що являє собою WLC? Які його функції та які види WLC існують?
3. Що таке VLAN та SSID?
4. Дайте визначення поняттю LightWeight Access Point?
5. Яка специфікація LWAPP?
6. Назвіть п’ять способів налаштування бездротової локальної мережі?
7. Які пристрої використовуються в топології Home Network to Access Internet?
8. Опишіть коротко про налаштування бездротових клієнтів?
9. Опишіть, як налаштовувати бездротовий контролер?