Лабораторна робота № 4

НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ БЕЗДРОТОВОЇ ЛОКАЛЬНОЇ МЕРЕЖІ побудованої з використанням безпровідних контролерів Cisco

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

Теоретичні відомості

Загальні теоретичні відомості про Wireless Lan Controller – WLC

WLC (*Wireless Lan Controller*) – використовується у поєднанні з протоколом точки доступу (LWAPP), для керування у великих кількостях адміністратором мережі або центром операцій з мережею. Контролер бездротової локальної мережі є частиною лінії даних в рамках бездротової моделі Cisco. Контролер WLAN автоматично обробляє конфігурацію бездротових точок доступу. Останнім десятиліттям Cisco WLC стали дуже популярними, оскільки компанії переходять від автономних дизайнів розгортання точок доступу (AP) до централізованого дизайну на основі контролерів, використовуючи переваги розширеної функціональності та резервування, що постачаються з використанням контролерів.

В даний час Cisco пропонує ряд різних моделей WLC, кожна з яких орієнтована на різні мережі. Як і очікувалося, більші моделі (WLC 8500, 7500, 5760 та ін.) Пропонують більше високошвидкісних мережних інтерфейсів гігабітного типу, високу доступність та деякі розширені функції, необхідні у великих та складних мережах, наприклад, підтримка більшої VLAN та Wi-Fi-мереж, тисячі AP & Клієнти на WLC-пристрої та багато іншого.

Останнім часом компанія Cisco почала пропонувати WLC-сервіси у більш високих комутаторах Catalyst шляхом вбудовування WLC всередині Catalyst Switches, наприклад Catalyst 3850, але також як віртуальний образ Virtual WLC, який працює під VMware ESX / ESXi 4.x / 5.x. Нарешті, маршрутизатори Cisco ISR G2 Series 2900 і 3900 можуть приймати модулі сервера Cisco UCS-E, додаючи функціональність WLC, підтримуючи до 200 точок доступу та 3000 клієнтів.

Рисунок 1 – Види моделей Wireless Lan Controller

Загальна характеристика одних 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. 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.

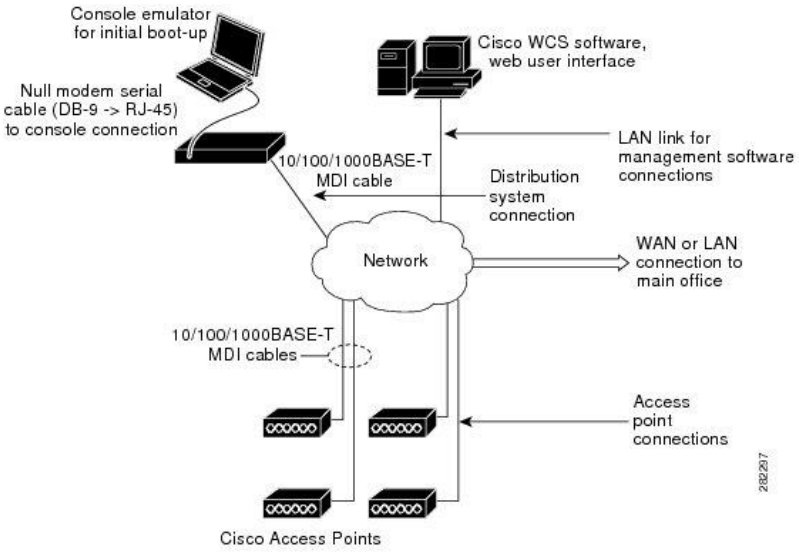

Рисунок 2 – Типова контролерна топологія та мережеві підключення

Загальна характеристика одних із видів WLC, серії 7500 та 8500

Бездротовий контролер серії Cisco 7500 – це високомасштабний контролер філіалу для бездротового розгортання декількох сайтів, в якому контролер об'єднується в центрі обробки даних. Контролер Cisco Flex 7500 може управляти бездротовими точками доступу у понад 500 відділеннях, що дозволяє IT-менеджерам налаштовувати, керувати та усунути помилки до 2 000 точок доступу та 20 000 клієнтів з даного центру. Бездротовий контролер серії Cisco Flex 7500 підтримує безпечний доступ до гостя, виявлення викрадень для відповідності платіжної картки (PCI) та роздільної здатності (локально включеного) голосового та відеозапису Wi-Fi.

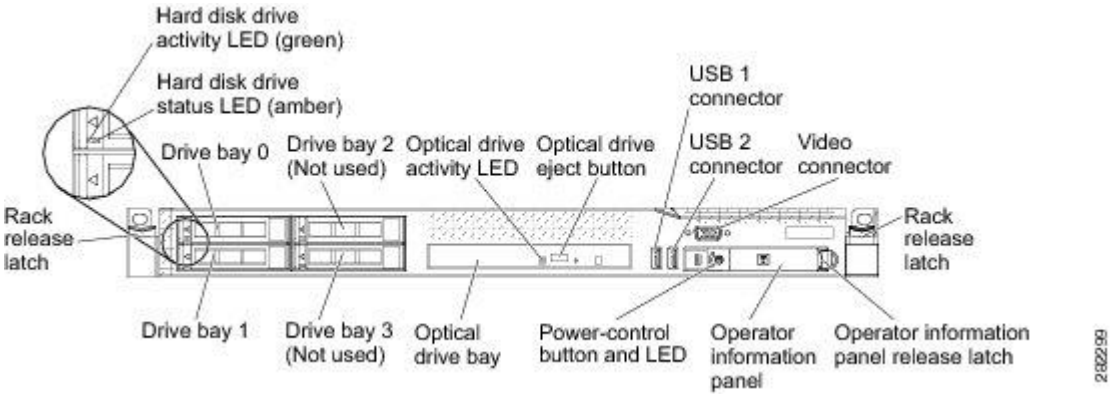

Рисунок 3 – Бездротовий контролер Cisco Flex 7500

Компоненти передньої панелі:

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

- світло діоди стану жорсткого диска: 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 диска s: кожен жорсткий диск із жорстким диском має індикатор активності, і коли цей індикатор блимає, це означає, що привід використовується.

- 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. Інформацію про елементи керування та світлодіодах на інформаційній панелі оператора див. На панелі інформації оператора.

- засувка для зняття інформаційної панелі оператора: Посуньте синю фіксатор ліворуч, щоб витягнути панель діагностики світлового шляху та переглянути світлодіоди та кнопки діагностики світлового шляху. Див. Панель діагностики світлового шляху для отримання додаткової інформації про діагностику світлового шляху.

- 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 послідовної консолі. 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 вдається, IMM вимикає світлодіоди, щоб допомогти вам діагностувати проблему, сповістити вас і 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 галузі 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, самоокупної мережі, яка дозволяє уникнути перешкод у системі РЧ;
- cisco ClientLink, для підвищення надійності та охоплення існуючих клієнтів.
- технологія Cisco ClientLink оптимізує мережеві мережі змішаного клієнта, допомагаючи гарантувати, що клієнти 802.11a / g та 802.11n працюють на максимально можливій швидкості.

Бездротовий контролер Cisco 8510 - це масштабована та гнучка платформа, яка забезпечує безперебійну роботу критично важливих мереж у широкомасштабних постачальника послуг та широкомасштабних розгортаннях. Бездротовий контролер Cisco 8510 може управляти бездротовими точками доступу у 6000 відділеннях і дозволяє IT-менеджерам налаштовувати, керувати та усунути неполадки до 6 000 точок доступу та 64 000 клієнтів з даного центру. Бездротовий контролер Cisco 8510 підтримує безпечний доступ до гостя, виявлення несправностей для відповідності платіжної картки (PCI) та голосових та відеозаписів вбудованих мереж Wi-Fi. Контролер Cisco 8510 може керувати централізованим (локальним режимом), режимом FlexConnect та розгортанням сітки в одному контролері.

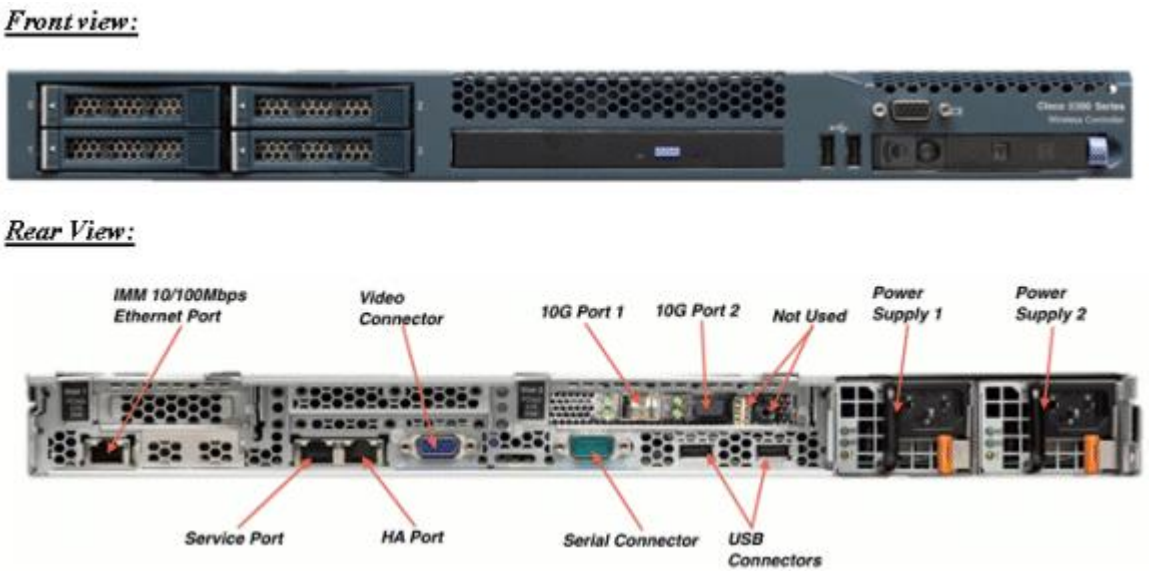

Рисунок 4 – Бездротовий контролер Cisco серії 8500 – 8510

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;
- підтримка зовнішньої підтримки;
- підтримка всіх режимів роботи АП (локальний, FlexConnect, монітор, детектор розвідників, Sniffer, та міст);
- не збиткова мобільність з мережею основних пакетів з впровадженням PMIPv6 MAG (RFC 5213);
- WFA Passpoint Certified (в процесі роботи - перевірте веб-сайт WFA для останнього статусу);
- 802.11r швидкий роумінг, двосторонній курс ліміту руху транспорту;
- відео потоку для мультимедійних потоків;
- ліцензування права на використання (RTU) для полегшення ліцензування та поточних операцій ліцензування;

Функції, які наразі не підтримуються на контрольній платформі 8500

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

Контролер Cisco 8500 дозволяє за замовчуванням переспрямовувати консоль із швидкістю 9600, що імітує термінал VT100 без керування потоком. Контролер 8500 має таку ж завантажувальну послідовність, що й існуючі контролери.

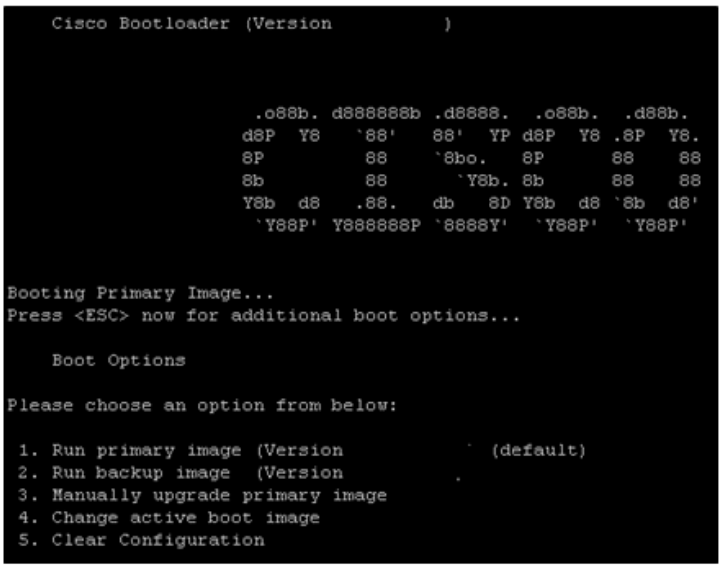

Рисунок 5 – Запуск бездротового контролера 8510

Загальні відомості про SSID та VLAN на WLC

Динамічні інтерфейси, також відомі як інтерфейси VLAN, створюються користувачами і розроблені таким чином, щоб бути аналогічними з VLAN для клієнтів бездротової локальної мережі. Контролер може підтримувати до 512 динамічних інтерфейсів (VLAN). Кожен динамічний інтерфейс індивідуально налаштований і дозволяє окремим потокам зв'язку існувати на будь-якому або всій порту розподільчої системи контролера. Кожен динамічний інтерфейс керує мережами VLAN та іншими зв'язками між контролерами та усіма іншими мережевими пристроями, і кожен виконує роль ретрансляції DHCP для бездротових клієнтів, пов'язаних з бездротовими локальними мережами (WLAN), зіставленими з інтерфейсом. Ви можете призначити динамічні інтерфейси для портів розподільних систем, мереж WLAN, інтерфейсу керування Layer 2 та інтерфейсу AP-manager Layer 3, і ви можете віднести динамічний інтерфейс до резервного порту. Також налаштувати нульовий, один або декілька динамічних інтерфейсів у порту розподільчої системи. Проте всі динамічні інтерфейси повинні бути в іншій підмережі VLAN або IP з усіх інших інтерфейсів, налаштованих на порту.

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 цю модель:

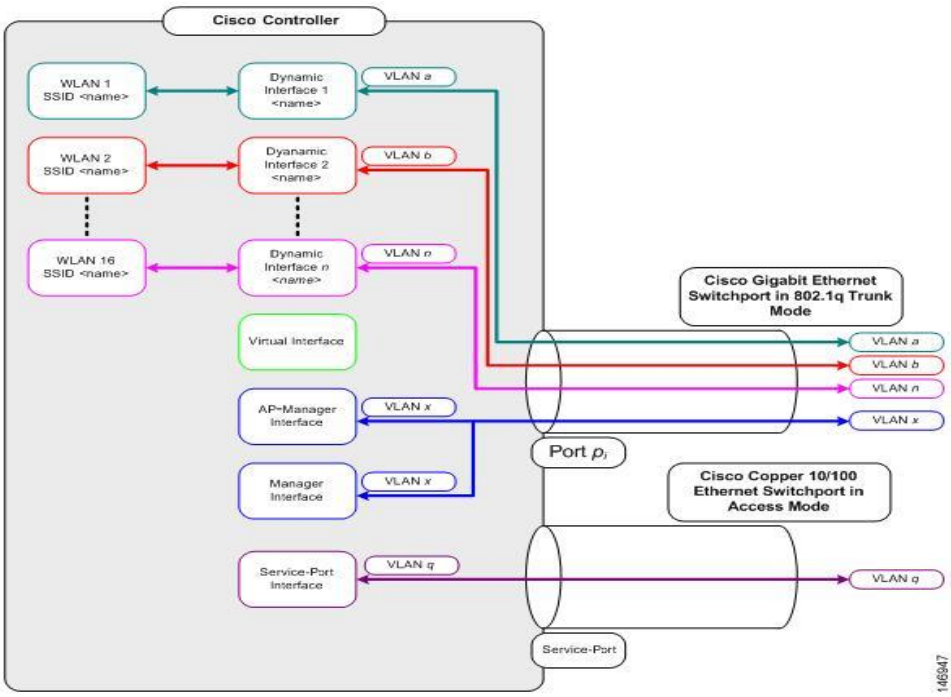

Рисунок 6 – Схематичний приклад VLAN, WLC

Під час налаштування на динамічному інтерфейсі контролера ви повинні використовувати теговані VLAN для динамічних інтерфейсів. Обмеження на налаштування динамічних інтерфейсів. Для налаштування динамічних інтерфейсів на контролері застосовуються такі обмеження: провідні 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 розмову; 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 — мережевий протокол TCP/IP стеку, що використовується у великих WLAN мережах. LWAPP забезпечує взаємодію бездротових точок доступу з одним або декількаами Wi-Fi контролерами.Основним завданням протоколу є автоматичне забезпечення бездротових точок доступу необхідними налаштуваннями для їх роботи у мережі, пов'язаних із SSID та параметрами, які надаються DHCP. У разі необхідності LWAPP надає точці доступу налаштування для побудови тунелю для трафіку користувачів мережі. Використання цього протоколу може допомогти системним адміністраторам великої WLAN скоротити час, що витрачається на налаштування, моніторинг та усунення несправностей. Також LWAPP є базисом для інструментів, що дозволяють аналізувати стан великої бездротової комп'ютерної мережі. 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) проектом IETF. AES-шифрування та режим лічильника з протоколом кодування автентифікації повідомлень з блокуванням шифрування блоків (CCMP) використовується для трафіку керування LWAPP.

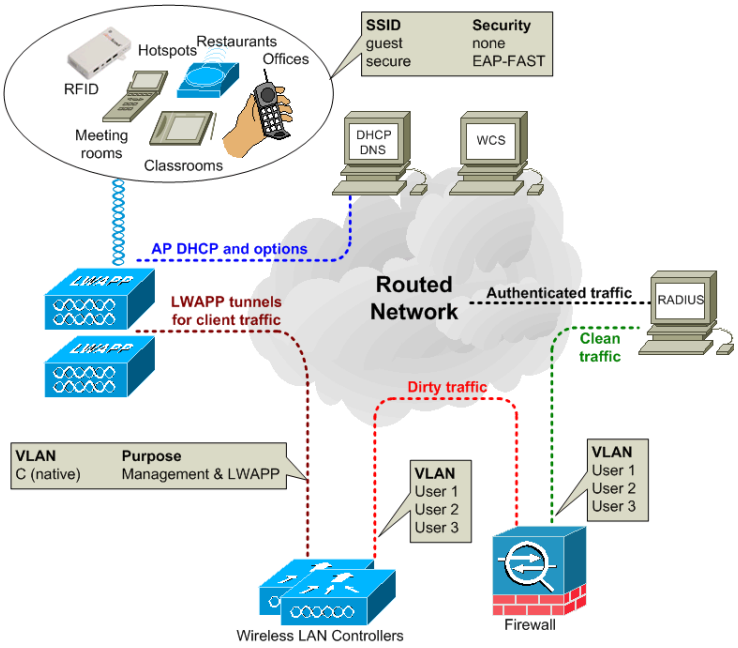

Рисунок 7 – Схематична побудова LightWeight Access Point

Операція LWAPP описується відповідно до топологічної схеми вище. Підключення клієнтського пристрою відбувається наступним чином: коли AP спочатку з'єднується з мережею, вона передає на шарі 2 шукає контролера. Це запит на пошук LWAPP, який повинен отримувати MAC-адреса керування контролером. Що має статися, контролер повинен відповісти за допомогою відповіді Discovery, що вказує кількість AP, пов'язаних з контролером. AP потім підключається до найменш завантаженого контролера, відправивши запит на приєднання. якщо на рівні 2 немає контролера, тоді AP запитує IP-адресу за допомогою DHCP. Якщо контролер не знаходиться в тій самій підмережі, мережа, що перемикається на шар 3, часто розгортає ретранслятор DHCP у мережах VLAN, які використовують AP. Сервер DHCP не тільки відповідає IP-адресою, але також надає ПС з IP-адресами доступних WLC (опція 43, під-варіант 241), ці адреси можуть бути пріоритетними, коли один контролер бездротової локальної мережі (WLC) є першим і другим Другий WLC Інформація про шлюз за замовчуванням та DNS також надається сервером DHCP. У режимі 3-го рівня AP надсилає запит на пошук LWAPP для IP-адреси менеджера AP за допомогою спрямованої трансляції. Якщо відповідь відсутній, AP надсилає запит на відкриття для будь-яких контролерів, які були вивчені з інших ПС через службу «По повітрю» (OTAP). Контролер реагує на відповідь Discovery, який вказує кількість ПП, пов'язаних з контролером. Потім AP надсилає до найменш завантаженого контролера запит на приєднання, який містить сертифікат AP.X.509.

AP використовує наступний порядок, коли зв'язується з контролером: спочатку спробуйте контролер Primary, потім Secondary, а потім третій контролер. Далі спробуйте майстер-контролер, тоді найменш завантажений контролер нарешті, найменш

завантажений інтерфейс диспетчера точок доступу WLC перевіряє AP, а потім надсилає відповідь приєднання LWAPP до AP, і це містить сертифікат X.509 WLC.

AP тепер перевіряє WLC, тим самим завершуючи процес пошуку та об'єднання, який включає в себе взаємне автентифікацію та висновок ключа шифрування, використовуючи сертифікати X.509. Це використовується для забезпечення процесу приєднання та майбутніх контро

льних повідомлень LWAPP. AP зареєстрований за допомогою WLC відповідно до параметрів апаратного забезпечення 60, які описують апаратний тип AP.

WLC оновлює програмне забезпечення зображення AP, якщо це потрібно, і налаштовує AP з відповідними настройками радіо та SSID. Клієнтський пристрій намагається підключити 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, куди може йти користувач, і що може зробити це користувач. 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 свого SSID. 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. Централізуючи інтелект у цих пристроях може бути безпека, мобільність, якість обслуговування (QoS) та інші функції, необхідні для роботи з WLAN – ефективно управляється по всій бездротовій компанії, крім того ще й шляхом розщеплення функцій між точкою доступу. Контролер IT-персоналу може спростити управління, підвищити продуктивність і підвищити безпеку великих бездротових мереж.

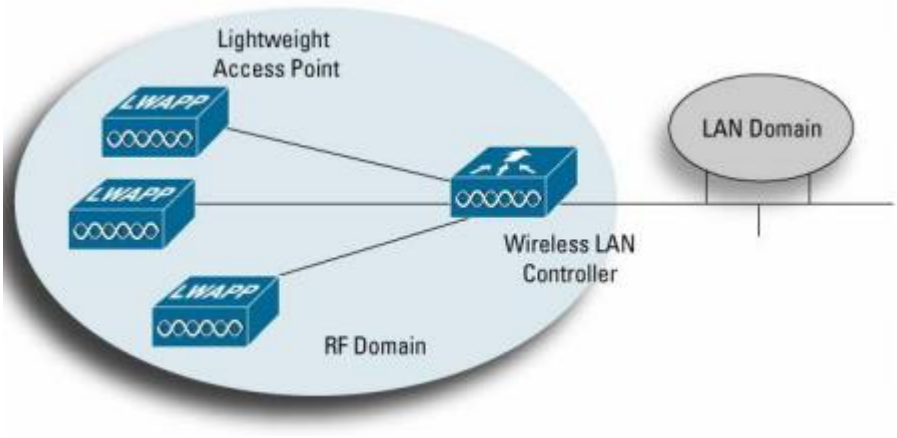

Рисунок 8 – WLAN системи централізованого інтелекту для широкого корпоративного управління підприємством та управління політикою

Традиційні рішення WLAN поширюють всю обробку трафіку, функції управління радіочастотним сигналом, безпеку та рухливість до точки доступу. Однак – це архітектура обмежує видимість трафіку 802.11 тільки для індивідуальної точки доступу. Це означає:

- індивідуальні точки доступу, коли вони використовуються без керуючого пристрою, повинні управлятися індивідуально, що може збільшити операційні витрати та кадрові потреби
- всесвітні атаки та перешкоди не видно в системі
- 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
- система не може корелювати чи передбачати активність на підприємстві
- обмежує можливість увімкнення оптимізованого балансу навантаження в реальному часі
- клієнти не можуть виконувати швидкі перекази, необхідні для підтримки додатків в режимі реального часу, таких як голос і відео.

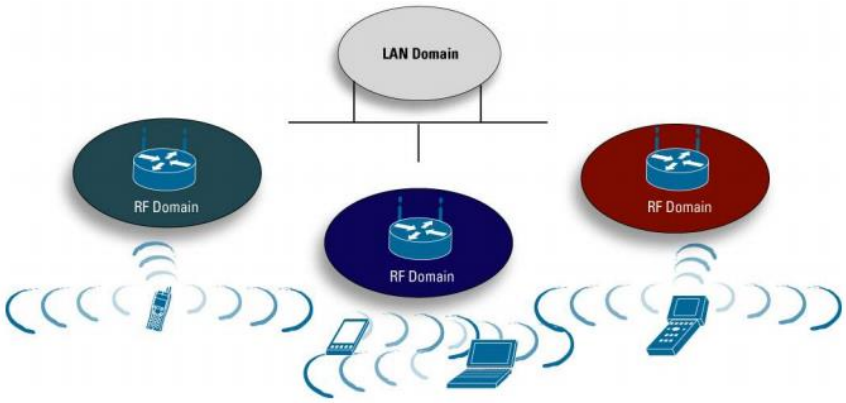

Рисунок 9' – Архітектура однорідної мережі WLAN обмежує продуктивність, керованість та безпеку

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 проект, 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:

- зменшить обсяг обробки в точці доступу, дозволяючи обмеженим обчислювальним ресурсам на цих пристроях зосередитися на бездротовій мережі доступ, на відміну від фільтрації та виконання політики
- включити схему, за допомогою якої централізована обробка трафіку, автентифікація, шифрування та виконання політики (QoS, безпека та ін.) Для цілого WLAN система

- забезпечити загальний механізм інкапсуляції та транспортування для взаємодії між точкою доступу з різноманітними джерелами через інфраструктуру рівня 2 або IP-маршрутизована мережа.

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. Відключити всі 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.
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 тегуванння для Native VLAN на транкових каналах та налагодити відкидання нетегованих кадрів.
8. Встановити стан порта/інтерфеса за замовчуванням як відключений

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 викори- стання 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*	ВиведенняінформаціїпроVLAN за її ідентифікатором(номером)

showvlanname *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
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 відмітності 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 рисунку 9.

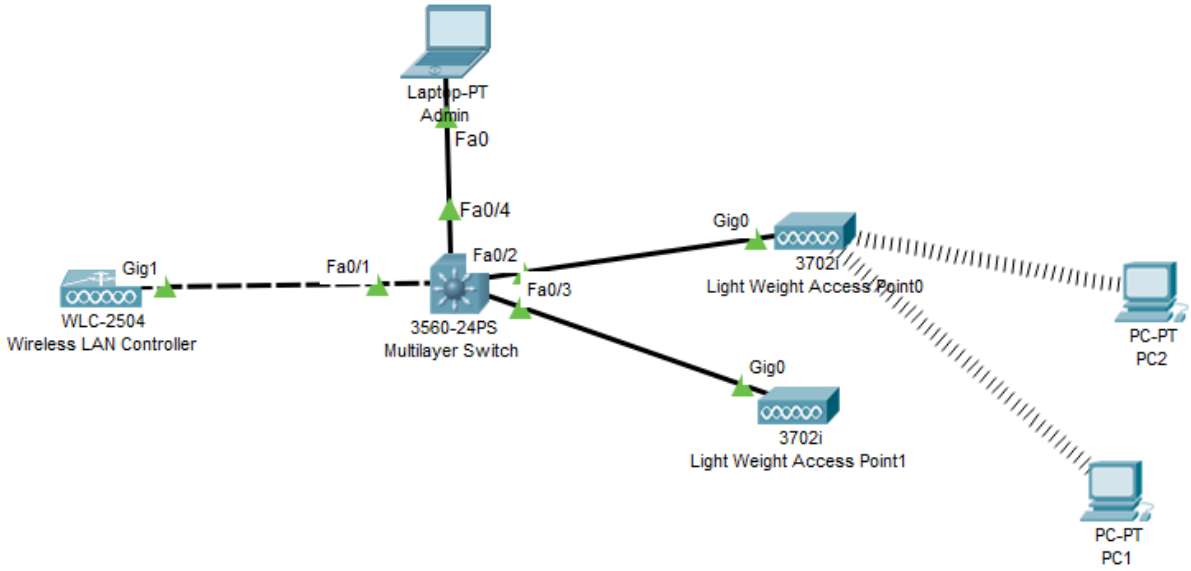

Рисунок 10 – Приклад налагодження Cisco WLC 2504

Під час побудови даної мережі для з'єднання пристроїв використано дані табл. 1. Для налагодження параметрів адресації пристроїв використано дані табл. 2.

Таблиця 2

Параметри інтерфейсів пристроїв для прикладу 2504

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Wireless Lan Controller	Gig1	L3-комутатор	Fa0/2
	Fa0/1		Fa0/3
			Fa0/4
L3-комутатор	Fa0/3	Wireless_0	Gig0
	Fa0/4	Wireless_1	Gig0
	Fa0/2	Laptop-PT	Fa0
Робоча станція WS_A_1	Wireless_0	L3-комутатор	Gig0
Робоча станція WS_A_2	Wireless_1		

Таблиця 3

Параметри адресації мережі WLC 2504

	WLC	Admin	Vlan
IP	192.168.1.200	192.168.1.100	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	8.8.8.8	8.8.8.8	—

Сценарії налагодження параметрів адресації інтерфейсів для Switch0 мережі наведені нижче.

Switch> enable
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
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 8.8.8.8
Switch(dhcp-config)# exit
Switch(config)# ip dhcp excluded-address 192.168.1.1
Switch(config)# ip dhcp excluded-address 192.168.1.100
Switch(config)# ip dhcp excluded-address 192.168.1.200
Switch(config)# service dhcp

Обираємо пристрій WLC 2504 (з WLC-PT є проблеми)

Перед налагодженням статично призначаємо робочій станції WLC_Admin ip-адресу 192.168.1.100, а для WLC 2504 ip-адресу 192.168.1.200.

Далі потрібно підключитись до WLC 2504, використовуючи веб-браузер ноутбука керування, використовуючи http://192.168.1.200 та 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 використовуйте протокол HTTP (незахищений) , а не HTTPS.

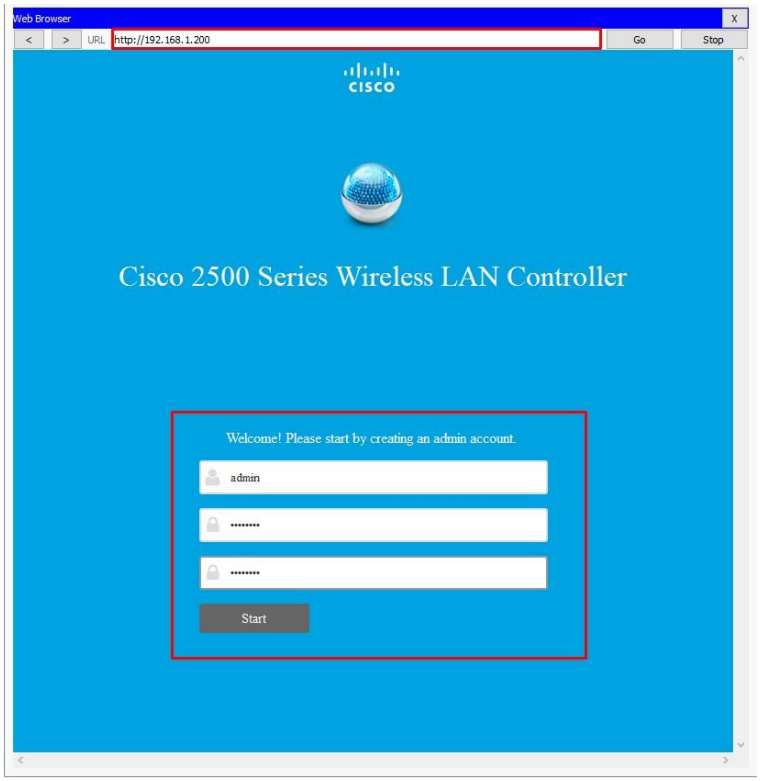

Рисунок 11 – Початкові налаштування Wirelles Lan Controller

Другий крок полягає в тому, щоб налаштувати час, розташування та керування IP-адресою WLC перед створенням першої захищеної бездротової мережі. Зверніть увагу, що функція "Гість-мережа" не підтримується Packet Tracer 7.1.1.

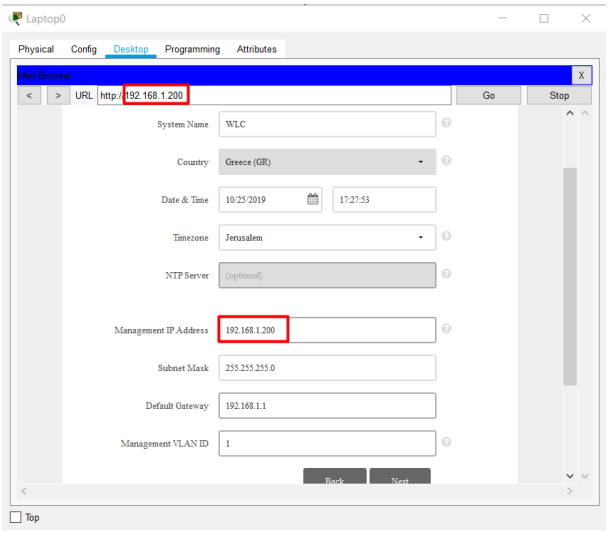

Рисунок 12.1 – Налаштування свого контролера

Після цієї початкової установки знову підключіться до Cisco WLC за допомогою HTTPS (https://192.168.1.254) . Якщо ви намагаєтеся підключитися за допомогою HTTP

(незахищені), WLC скидає підключення, але не автоматично переспрямовує з'єднання з URL-адресою HTTPS. Далі після натискання кнопки «next», перед нами повинно відкритися вікно з власними налаштуваннями.

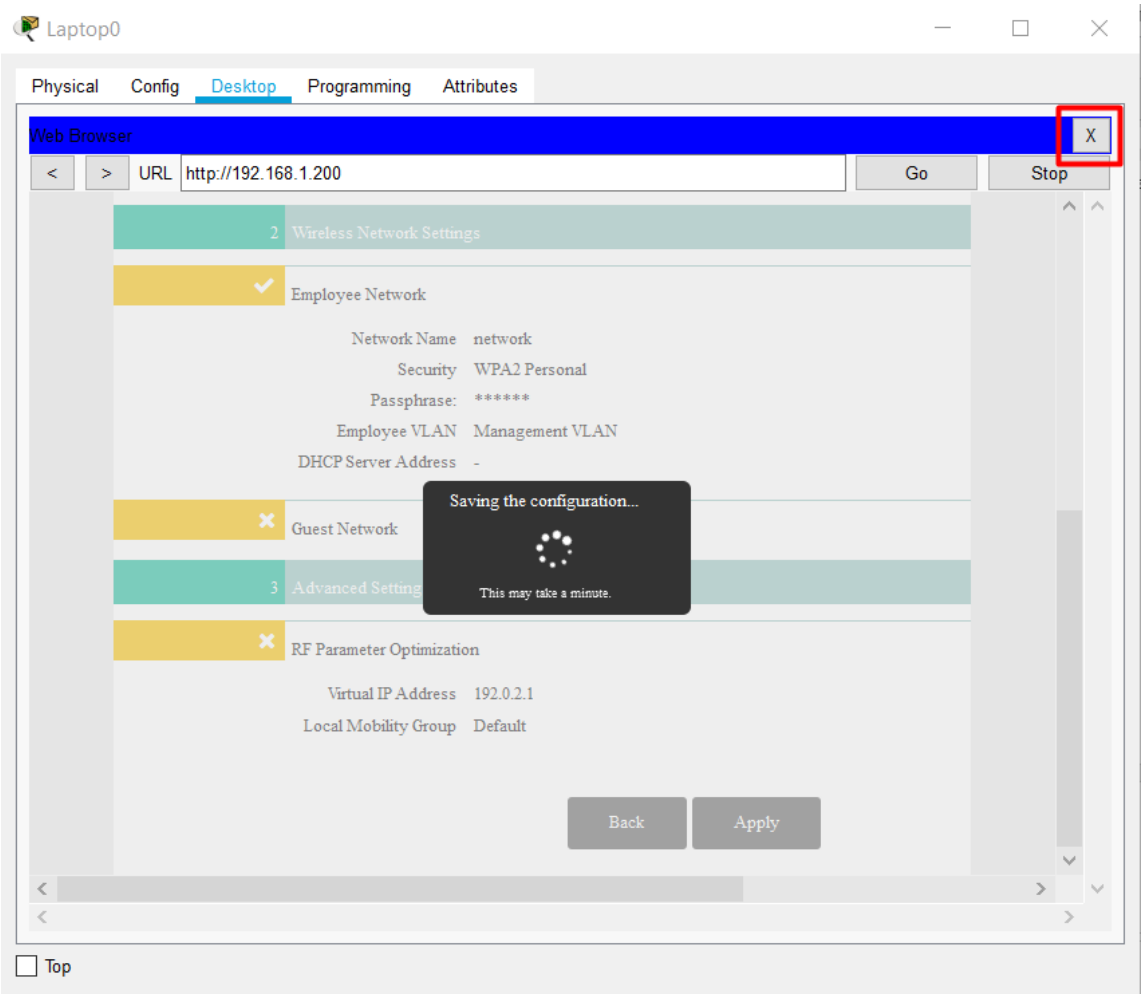

Рисунок 12.2 – Поява напису про зберігання конфігурації

При появі напису на рисунку 13 не потрібно чекати завершення збереження конфігурації, натисніть на крестик для повернення у меню та оберіть Command Prompt для перевірки зв’язку з налагодженним WLC.

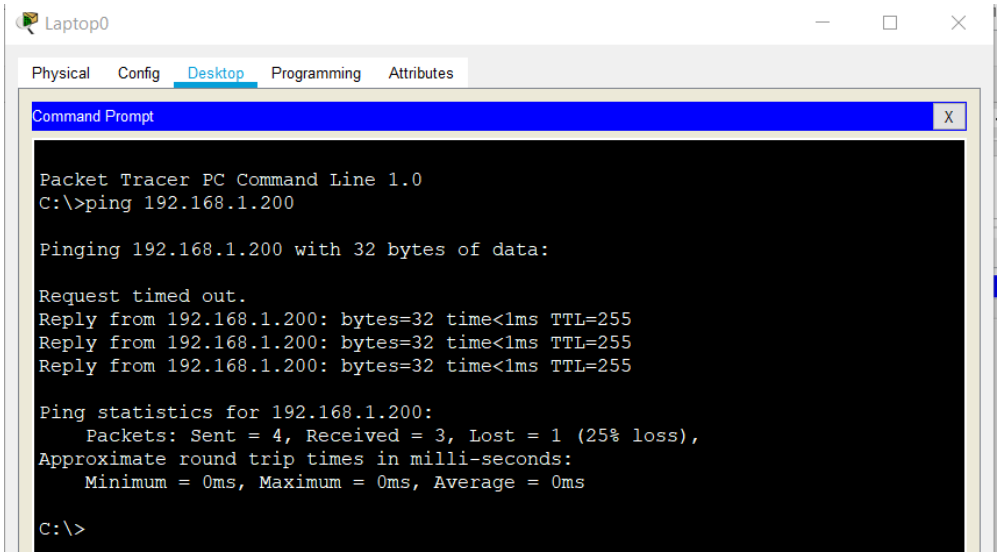

Рисунок 12.3 – Перевірка зв'язку.

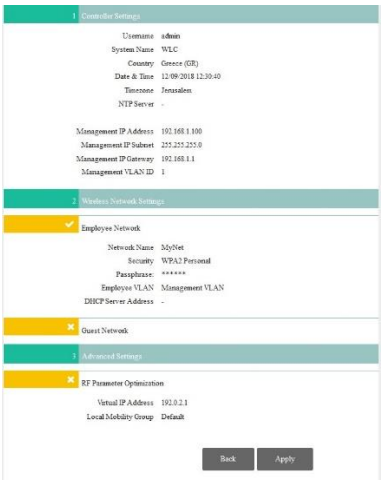

Рисунок 13 – Завершальний процес застосування

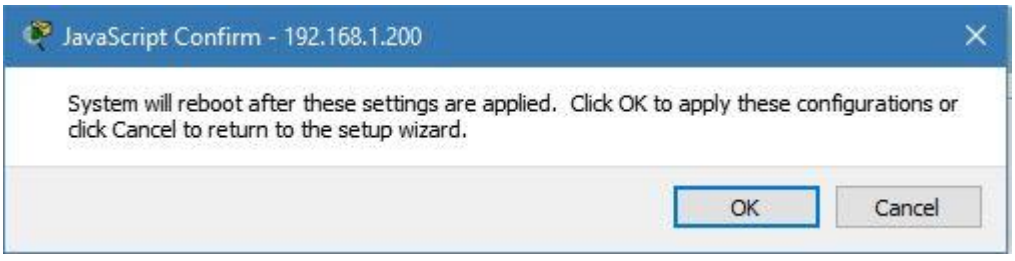

Рисунок 14 – Перед підключення до контролеру

На данім із етапів потрібно зачекати певний час, тому що відбувається самий процес перезапуску контролера.

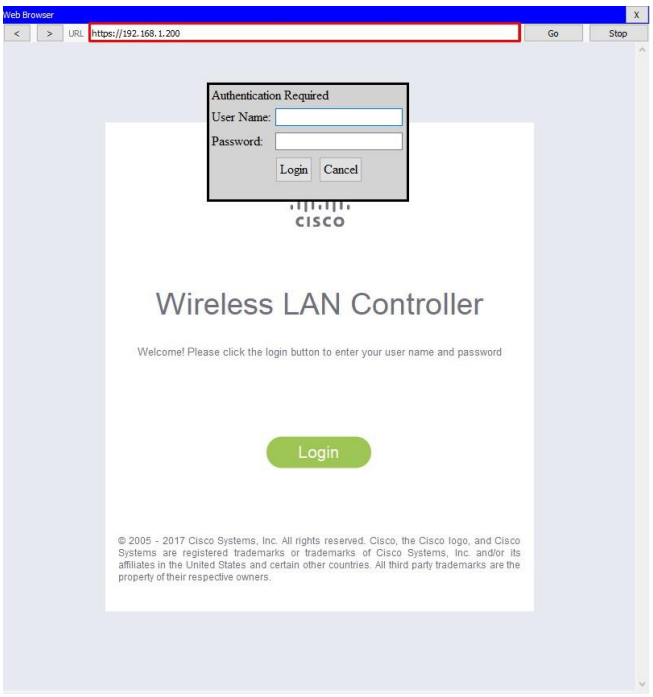

Рисунок 15 – Входження у систему WLC

В попередніх етап ми вказали логін та пароль, при вході – зазвичай по замовчуванню встановлюємо логін: admin, пароль: admin.

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

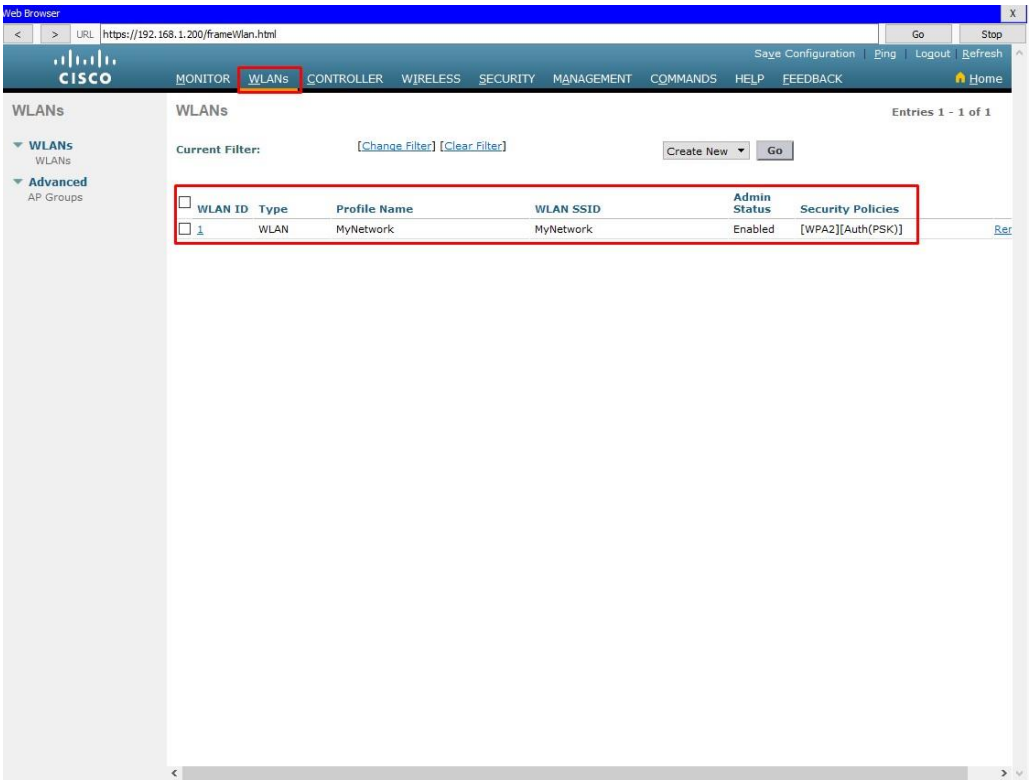

Рисунок 16 – Створення WLAN

WLC відображає успішно зареєстровані точки доступу з цією IP-адресою. докладні дані недоступні, оскільки ця функція не була реалізована в Packet Tracer 7.1

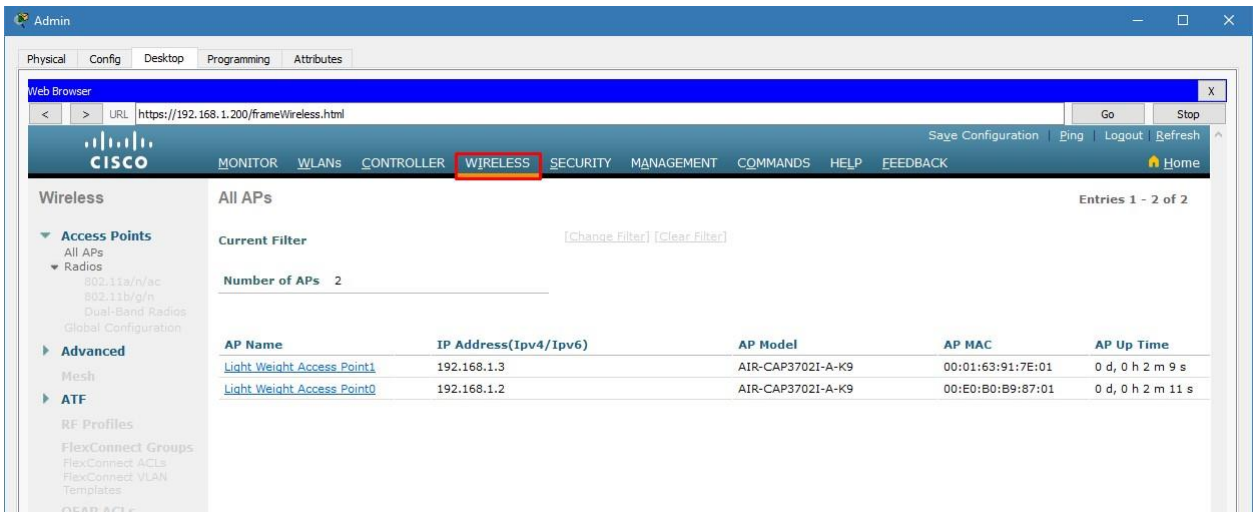

Рисунок 17 – Успішно зареєстровані точки доступу

Завдання на лабораторну роботу

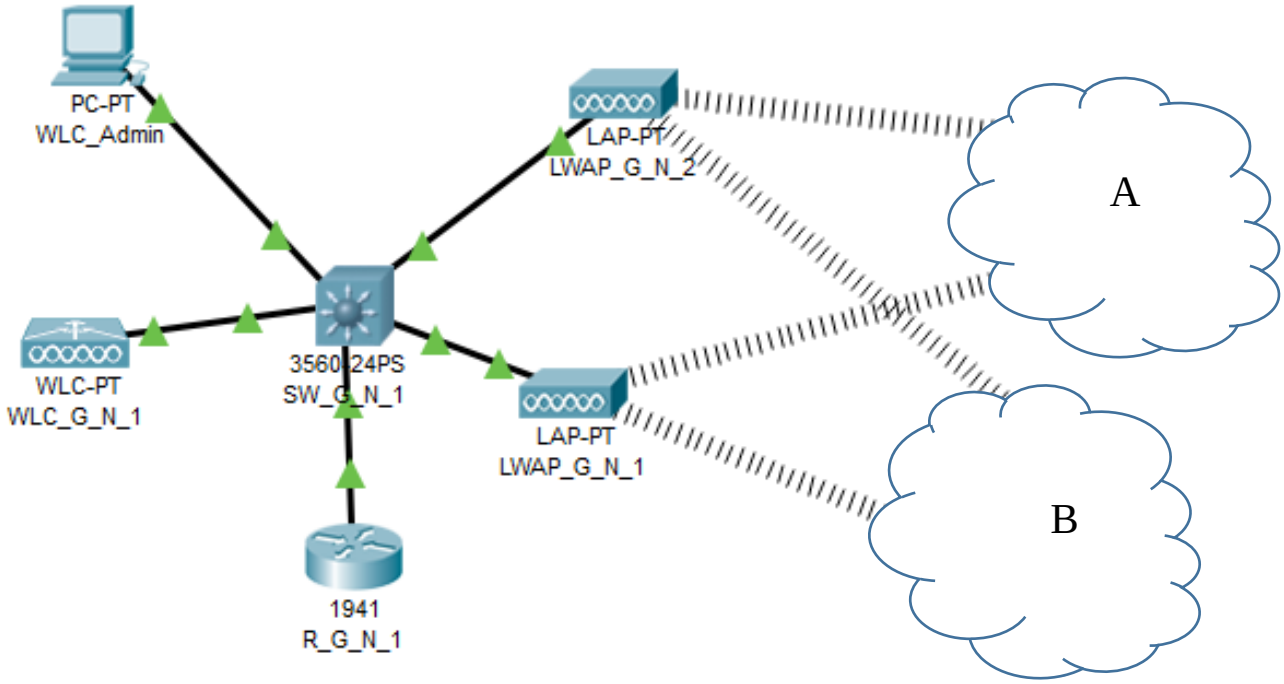

Рисунок 18 – Проект мережі Wireless Lan Controller

1. У середовищі програмного симулятора/емулятора створити проект мережі (рис. 17). Під час побудови мережі звернути увагу на вибір моделей мережних пристроїв, мережних модулів та адаптерів, а також мережних з'єднань. Кількість робочих станцій та для побудованої мережі заповнити описову таблицю, яка аналогічна табл. 1.
2. Розробити схему адресації пристроїв мережі. Для цього скористатися даними табл. 4. Результати навести у вигляді таблиці, яка аналогічна табл. 3.

3. У побудованій мережі налагодити функціонування WLC на основі групування портів (номер та назва VLAN керування зазначені у табл. 5, номери та назви VLAN користувачів зазначені у табл. 6). Виконати додаткові налагодження, які забезпечать підвищення рівня захищеності побудованої мережі.

4. Налагодити можливість LightWeight Access Point**.**

5. Дослідити особливості та отримання службової та діагностичної інформації про налагоджені WLC.

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	Аутентифікація R_G_N_2
1	819	WEP
2	829	WPA2-PSK
3	2911	Open
4	819	WPA2-PSK
5	829	Open
6	2911	WEP
7	819	Open
8	829	WEP
9	2911	WPA2-PSK
10	819	WEP
11	829	WPA2-PSK
12	2911	Open
13	819	WPA2-PSK
14	829	Open
15	2911	WEP
16	819	Open
17	829	WEP
18	2911	WPA2-PSK
19	819	WEP
20	829	WPA2-PSK
21	2911	Open

22	819	WPA2-PSK
23	829	Open
24	2911	WEP
25	819	Open

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 їх є?
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 комутатор?