ЗАТВЕРДЖЕНО

Науково-методичною радою
Державного університету
«Житомирська політехніка»

протокол від ___ _____ 2024 р.
№ ___

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
для проведення лабораторних робіт з навчальної дисципліни «БЕЗДРОТОВІ МЕРЕЖІ»

для здобувачів вищої освіти освітнього ступеня «бакалавр»

факультет інформаційно−комп’ютерних технологій

кафедра комп’ютерної інженерії та кібербезпеки

Рекомендовано на засіданні
кафедри комп’ютерної інженерії
та кібербезпеки
26 серпня 2024 р.,
протокол № 6

Розробники: к.т.н., доц. кафедри КІ та КБ РОССІНСЬКИЙ Юрій
ст. викл. кафедри КТуМтаТ МОРОЗОВ Дмитро
асистент кафедри КІ та КБ ХОХЛОВ Михайло

Житомир
2024

ЗМІСТ

Лабораторна робота №1. Перетворювання одиниць вимірювання в бездротових мережах…..... 3

Лабораторна робота №2. Налагодження та дослідження функціонування бездротових мереж на базі маршрутизаторів CISCO LINKSYS ……..... 7

Лабораторна робота №3. Налагодження та дослідження роботи бездротових мереж, побудованих на базі маршрутизаторів CISCO ……..……... 30

Лабораторна робота №4. Налагодження та дослідження роботи бездротової локальної мережі побудованої з використанням бездротових контролерів Cisco…..... 57

Лабораторна робота №5. Налагодження та дослідження роботи CISCO MERAKI 85

Лабораторна робота №6. Моделювання роботи «розумного» будинку в середовищі Cisco Packet Tracer……..... 104

Лабораторна робота №7. Візуальне програмування мікроконтролерів в Cisco Packet Tracer 123

Лабораторна робота №8. Дослідження керування IoT пристроїв через мережу провайдера 137

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ..... 142

Лабораторна робота №1. Перетворення одиниць вимірювання в бездротових мережах

Метою даної лабораторної роботи є знайомство з одиницями вимірювання потужності сигналу в бездротових мережах і основними діями над ними.

Завдання на лабораторну роботу:
• Переведіть потужність передавача з мВт в дБм;
• Переведіть потужність передавача з дБм в мВт.

Теоретична частина:

Потужність сигналу в бездротових мережах є ключовим фактором, що впливає на якість зв'язку та продуктивність мережі. Одним з важливих аспектів є відстань, на яку сигнал може бути переданий. Зазвичай, чим вища потужність сигналу, тим далі він може досягати, проте в реальних умовах існує безліч завад, як фізичних, так і абстрактних. В бездротових мережах можуть виникати завади з інших пристроїв, які працюють на тій же або сусідніх частотах. Це може призводити до зниження якості зв'язку. Для боротьби з цими проблемами використовують технології, такі як адаптивне регулювання потужності передачі або методи розподілу частот.

Крім того, важливо звертати увагу на енергоефективність. Багато сучасних бездротових технологій, зокрема Wi-Fi 6 та 5G, розроблені з урахуванням енергоефективності, що дозволяє зменшити споживання енергії без шкоди для продуктивності. Це особливо важливо для мобільних пристроїв, які працюють від акумуляторів.

Регуляторні норми також впливають на потужність сигналу в бездротових мережах. В різних країнах існують обмеження на максимальну потужність передавачів, що необхідно враховувати під час проектування та розгортання мережі. Це допомагає запобігти завадам між різними бездротовими системами та забезпечити безпечне використання радіочастотного спектру.

При розрахунку параметрів бездротових мереж зазвичай доводиться виконувати перетворювання одних одиниць вимірювання в інші. В технічних описах і законодавчих актах, що регулюють використання радіочастотного спектру в Україні, присутні як лінійні (вати, Вт), так і логарифмічні (децибели, дБ) одиниці вимірювання.

Основна мета перетворення одиниць вимірювання в бездротових мережах — це забезпечення точності та зрозумілості даних. Мережеві адміністратори можуть порівнювати продуктивність різних технологій, таких як Wi-Fi, LTE або 5G, використовуючи одні й ті ж одиниці вимірювання. Це допомагає в ухваленні

рішень щодо оптимізації мережі та вибору відповідного обладнання, що, в свою чергу, підвищує загальну ефективність мережевих рішень.

Одиниці вимірювання потужності сигналу в бездротових мережах зазвичай виражаються в децибелах (дБ) або децибелах від міліват (дБм). Децибели є логарифмічною одиницею, яка дозволяє зручно представляти широкі діапазони потужності сигналу. Наприклад, потужність сигналу в 1 мВт відповідає 0 дБм, а 10 мВт — 10 дБм. Це перетворення спрощує обчислення і порівняння, адже замість роботи з великими числовими значеннями, ми використовуємо менші, більш зручні для сприйняття величини. В децибелах прийнято вимірювати затухання хвилі при розповсюдженні їх в середовищі поглинання, коефіцієнт підсилення антени, відношення сигнал/шум.

Для оцінки потужності сигналу, що виражена в дБ, необхідно обчислити співвідношення:

$$P_{dB} = 10\lg\frac{P_1}{P_0}, \qquad (1.1)$$

де, P_1 – виміряна потужність; P_0 – потужність, що прийнята за основу.

На відміну від безрозмірного децибелу для виразу абсолютних значень потужності використовуються величини dBm (дБм) і dBW (дБВт). Для їх використання необхідно визначити, який рівень фізичної величини, що вимірюється буде прийнято за базовий (умовний 0 дБ).

В dBm (дБм) зазвичай виражається потужність передавача. За нульовий рівень дБм прийнята потужність 1мВт. Для переводу потужності з мВт в дБм необхідно виконати наступний вираз:

$$P_{dBm} = 10\lg\frac{P_{mW}}{1mW}, \qquad (1.2)$$

де P_{dBm} - потужність передавача, виражена в дБм; P_{mW} – потужність передавача, виражена в мВт.

Зворотне перетворення з дБм в мВт виконується за наступною формулою:

$$P_{mW} = 10^{\frac{P_{dBm}}{10}}. \qquad (1.3)$$

В dBW (дБВт) за нульовий рівень прийнято потужність 1 Вт. Формули для переводу аналогічні вищезазначеним з тією різницею, що в якості нульового рівня обрана величина 1 Вт, а виміряна потужність також повинна виражатися в ватах.

Величина dBi (дБі) називається ізотропний децибел (децибел відносного ізотропного випромінювача і характеризує коефіцієнт підсилення антени відносно коефіцієнта направленої дії ізотропного випромінювача. Як правило, якщо не зазначено спеціально, характеристики підсилення реальних антен даються саме відносно підсилення ізотропного підсилювача.

Децибели є нелінійними одиницями вимірювання. Тому, коли кажуть, наприклад про подвоєння потужності рівної 100 мвт (20 дБм), це не означає, що потужність збільшилась до 40 дБм. 40 дБм відповідає 10000 мВт. Збільшення потужності (в мВт) в 2 рази еквівалентно додаванню до потужності (в дБм) 3 дБм. Зменшення потужності в мВт в 2 рази еквівалентно відніманню з потужності в дБм 3 дБм. Відповідно, при збільшенні потужності 100 мВт в 2 рази, необхідно додати 20 дБм і 3 дБм та отримати потужність 23 дБм.

Хід роботи:

1. Вкажіть значення дБм для кожного з наступних рівнів потужності, виражених в мВт. За нульовий рівень дБм прийміть потужність в 1мВт. Округліть значення до цілої частини.

Потужність передавача, мВт	Потужність передавача, дБм
97	20
15	
37	
63	
420	
160	
1,6	
250	
900	
2	

Для виконання завдання потрібно підставити значення потужності передавача в мВт в формулу (1.2). Наприклад:

$$10\lg\frac{97}{1} = 20$$

2. Вкажіть значення мВт для кожного з наступних рівнів потужності, що виражені в дБм. Округліть отримане значення до цілої частини.

Потужність передавача, дБм	Потужність передавача, мВт
16	40
30	
2	
40	
36	
33	
0	
28	
9	
31	

Для виконання завдання потрібно підставити значення потужності передавача в дБм в формулу (1.3). Наприклад:

$$10^{\frac{16}{10}} = 40 \text{ мВт}.$$

3.1. Потужність передавача 200 мВт зменшилась в 4 рази. Обчисліть нове значення потужності та вкажіть його в дБм.

3.2. Потужність передавача 63 мВт збільшилась в 32 рази. Обчисліть нове значення потужності та вкажіть його в дБм.

3.3. Потужність передавача 10 мВт зменшилась в 10 разів. Обчисліть нове значення потужності та вкажіть його в дБм.

3.4. Потужність передавача 158 мВт зменшилась в 5 разів. Обчисліть нове значення потужності та вкажіть його в дБм.

3.5. Потужність передавача 1000 мВт зменшилаьс в 10 разів. Обчисліть нове значення потужності та вкажіть його в дБм.

3.6. Потужність передавача 200 мВт збільшилась в 6 разів. Обчисліть нове значення потужності та вкажіть його в дБм.

3.7. Потужність передавача 40 дБм зменшилась в 100 разів. Обчисліть нове значення потужності та вкажіть його в дБм.

3.8. Потужність передавача 30 дБм зменшилась в 1000 разів. Обчисліть нове значення потужності та вкажіть його в дБм.

3.9. Потужність передавача 20 дБм зменшилась в 2 рази. Обчисліть нове значення потужності та вкажіть його в дБм.

3.10. Потужність передавача 16 дБм збільшилась в 4 рази. Обчисліть нове значення потужності та вкажіть його в дБм.

Лабораторна робота №2. Налагодження та дослідження функціонування бездротових мереж на базі маршрутизатоів CISCO LINKSYS.

Мета роботи: навчитися налаштовувати та підключати бездротові мережі; налагодити захист бездротової мережі за допомогою WAP-ключа; налаштувати статичну маршрутизацію на маршрутизаторі Linksys.

Теоретичні відомості

Загальні відомості про виробника

Linksys від Cisco, широко відома як Linksys, є торговою маркою мережевих продуктів для домашніх мереж та мереж малих офісів. Зараз продукція виробляється від Cisco Systems, раніше Linksys була незалежною компаніэю, заснованою в 1995 році, перш ніж була придбана Cisco в 2003 році.

На даний час, продукти, як і раніше, розповсюджуються під назвою бренду Linksys та включають в себе лінійку приладів широкосмугового доступу і бездротових маршрутизаторів, Ethernet комутаторів, VoIP-обладнання, бездротових IP-камер, цифрових аудіо, мережевих систем зберігання даних тощо.

Одним із яскравих прикладів сучасних рішень Linksys для бездротових мереж можна вважати Mesh-систему Linksys Velop, пристрої якої зображені на рис. 2.1.

Рисунок 2.1 – Пристрої лінійки Linksys Velop

Linksys Velop — це система Wi-Fi Mesh, яка забезпечує безперебійне бездротове з'єднання на великих територіях. Вона складається з декількох модулів, які взаємодіють один з одним, формуючи єдину мережу. Ця технологія дозволяє забезпечити стабільне покриття без мертвих зон, що особливо важливо в приміщеннях з товстими стінами або великою площею. Завдяки можливості масштабування, користувачі можуть легко додавати нові вузли для покращення покриття.

Однією з основних переваг Linksys Velop є простота налаштування та управління. Користувачі можуть легко налаштувати систему за допомогою мобільного додатку, який пропонує інтуїтивно зрозумілий інтерфейс. Це дозволяє не лише налаштовувати мережу, але й моніторити її в реальному часі, керувати підключеннями пристроїв та встановлювати обмеження на швидкість для гостьових мереж.

Linksys Velop також підтримує новітні стандарти бездротового зв'язку, такі як Wi-Fi 6, що забезпечує високу швидкість передачі даних та надійність з'єднання. Це особливо важливо в умовах, коли одночасно підключено багато пристроїв. Система також має вбудовані функції безпеки, такі як WPA3, що забезпечують додатковий захист даних. Завдяки своїм потужним характеристикам і технологічним інноваціям, Linksys Velop є відмінним вибором для тих, хто шукає надійне та ефективне рішення для бездротового з'єднання.

На жаль, дана серія обладнання не представлена в симуляторі Packet Tracer.

Одним з відомих представників Linksys є також серія простих і водночас потужних бездротових маршрутизаторів Linksys WRT.

Загальні відомості про маршрутизатор Linksys WRT300N

Linksys WRT300N – це широкосмуговий маршрутизатор Wireless-N, який використовує технологію бездротової мережі під назвою Multiple Input Multiple Output (MIMO). Технологія MIMO використовує кілька радіоприймачів, щоб забезпечити надійний сигнал, який проходить до чотирьох разів далі і зменшує мертві плями.

Зовнішній вигляд маршрутизатора наведено на рис. 2.1.

Зовнішній вигляд задньої панелі маршрутизатора наведено на рис. 2.2.

Зовнішній вигляд передньої панелі маршрутизатора наведено на рис. 2.3.

Призначення портів маршрутизатора наведені у табл. 1.

Призначення портів маршрутизатора наведені у табл. 2.

Основні характеристики маршрутизатора наведені у табл. 3.

Рисунок 2.1 − Зовнішній вигляд маршрутизатора Linksys WRT300N

Рисунок 2.2 − Зовнішній вигляд задньої панелі маршрутизатора Linksys WRT300N

Таблиця 1

Призначення портів маршрутизатора Linksys WRT300N

	**Internet** - інтернет-порт, за допомогою якого можна підключити маршрутизатор до глобальної мережі.
	**Ethernet 1, 2, 3, 4** - Ці порти призначені для підключення пристроїв локальної мережі.
	**Reset**- Є два способи скинути Linksys WRT300N до заводських налаштувань за замовчуванням. Або тримати натисненою кнопку «RESET» впродовж 10 секунд або відновити значення за замовчуванням через веб-меню: **Administration > Factory Defaults**.
	**Power** – роз’єм підключення адаптера живлення. Для вимкнення пристрою достатньо знеструмити адаптер або від’єднати штекер живлення.

Рисунок 2.3 − Зовнішній вигляд передньої панелі маршрутизатора Linksys WRT300N

Таблиця 2

Призначення індикаторів маршрутизатора Linksys WRT300N

	**Power (Green) -** Індикатор живлення, має бути активний при увімкненому пристрої.
	**Ethernet 1, 2, 3, 4** – Індикація наявності підключених пристроїв локальної мережі до відповідних портів на задній панелі даного маршрутизатора. Мають два стани: 1) Постійно активний – пристрій підключено до порту. 2) Блимає – є активна передача даних через порт.
	**Reset –** Індикатор успішного скидання маршрутизатора до заводських налаштувань.
	**Wireless** – Індикатор роботи вбудованої бездротової точки доступу.
	**Security (Green) -** Індикатор безпеки, активний при увімкненій функції захисту бездротової мережі.

Таблиця 3

Основні характеристики маршрутизатора Linksys WRT300N

ЗАГАЛЬНІ	
Частотний діапазон	2.4 GHz
Метод аутентифікації	RADIUS, Radio Service Set ID (SSID)
Індикатори стану	Port status, power, link OK, link/activity
Алгоритм шифрування	128-bit WEP, 64-bit WEP, WPA, WPA2
Протокол маршрутизації	Static IP routing
Виробник	Cisco Systems
МОДЕМ	
Кількість антен	3
ЖИВЛЕННЯ	
Тип	зовнішній адаптер живлення
МЕРЕЖА	
Форм-фактор	desktop
Тип	wireless router
Технологія підключення	дротова, бездротова
Протокол передачі даних	Ethernet, Fast Ethernet, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (draft)

Продовження табл. 3

Мережевий / транспортний протокол	IPSec, L2TP, PPPoE, PPTP
Особливості	256-bit encryption,
	Access Point operational mode, firewall protection, firmware upgradable, full duplex capability, DHCP support, DMZ port, MAC address filtering, MDI/MDI-X switch, MIMO technology, NAT support, Stateful Packet Inspection (SPI), VPN passthrough
Стандарти	IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (draft), IEEE 802.3, IEEE 802.3u
Бездротовий протокол	802.11b/g/n (draft)
Протокол маршрутизації	static IP routing
Протокол перемикання	Ethernet
Протокол дистанційного керування	HTTP, HTTPS
Кількість wan портів	1
Інтегрований комутатор	4-port switch
Ключові особливості	VPN support, firewall
АНТЕНА	
Кількість	3
Рівень посилення	2 dBi
ІНТЕРФЕЙС	
Тип	network
Інтерфейс	Ethernet 10Base-T/100Base-TX
Кількість	1, 4
Тип роз'єму	RJ-45
WAN / DMZ	WAN
Тип	LAN, WAN

Порядок налагодження маршрутизатора Linksys

Налагодження роботи маршрутизатора Linksys згідно з рекомендаціями виробника складається із певних обов'язкових та необов'язкових етапів. Порядок виконання згаданих етапів є таким:

1. Під'єднайте відповідний кабель з робочої станції до порту Ethernet 1 на маршрутизаторі Linksys;
2. Дочекайтеся, коли індикатор зв'язку зміниться на зелений. Потім відкрийте вікно командного рядка робочої станції. За допомогою команди ipconfig перевірте IP-адресу, призначену робочій станції;
3. За допомогою команди ping 192.168.0.1 перевірте, чи має вузол Host-A доступ до шлюзу за замовчуванням;
4. Для налаштування маршрутизатора Linksys за допомогою графічного інтерфейсу користувача потрібно відкрити його в веб-браузері. Відкрийте веб-браузер та виконайте підключення до маршрутизатора, ввівши в адресному рядку адресу шлюзу.
5. Введіть ім'я користувача admin та аналогічний пароль для доступу до маршрутизатора Linksys;
6. Для параметра Internet Connection Type (Тип підключення до Інтернету) виберіть одне із запропонованих значень з спадного списку: Static IP, PPPoE або Automatic configuration–DHCP;
7. Прокрутіть сторінку вниз до кінця і натисніть кнопку Save Settings (Зберегти параметри). При переході між вкладками без збереження налаштовані параметри будуть втрачені;
8. Відкрийте вкладку Wireless (Бездротові мережі) і вивчіть параметри зі списку Network Mode (Режим мережі). Змініть SSID на, наприклад, MyHomeNetwork;
9. Натисніть кнопку Save Settings, а потім – Continue;
10. Перейдіть до вкладки Wireless Security під вкладкою Wireless. Встановіть для параметра Security Mode значення WPA2 Personal.

Модельний приклад налагодження маршрутизатора Linksys зі статичним типом з'єднання з інтернетом в Cisco Packet Tracer

Розглянемо специфіку налагодження мережі на базі маршрутизатора Linksys, схему якої наведено на рис. 2.4.

Граничним маршрутизатором було обрано пристрій Cisco Router 2911.

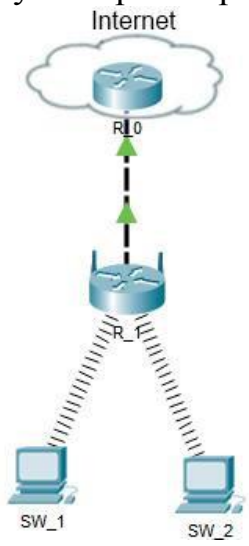

Рисунок 2.4 − Топологія мережі

Під час побудови мережі для з'єднання пристроїв використано дані табл. 4. Для налаштування параметрів адресації пристроїв використано дані табл. 5.

Таблиця 4

Параметри з'єднань пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R_1	Internet	Cloud	Gig0/0
	Wireless	Робоча станція WS_1	Wireless0
	Wireless	Робоча станція WS_2	Wireless0
Робоча станція WS_1	Wireless0	Маршрутизатор R_1	Wireless
Робоча станція WS_2	Wireless0	Маршрутизатор R_1	Wireless

Таблиця 5

Параметри адресації мереж для прикладу

Підмережа/ Пристрій	Інтерфейс/ Мережевий адаптер/ Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа A	-	175.0.1.0	255.255.255.252	/30
Підмережа B	-	192.168.0.0	255.255.255.0	/24
Маршрутизатор R_1	Internet	175.0.1.2	255.255.255.252	/30
	Wireless	192.168.0.1	255.255.255.0	/24
Робоча станція WS_1	Мережевий адаптер	192.168.0.2	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.0.1		

Продовження табл. 5

Робоча станція WS_2	Мережевий адаптер	192.168.0.2	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.0.1		

Сценарій налагодження маршрутизатора R_1 зі статичним типом з'єднання з мережею інтернет наступний:

1. Налаштування IP-адреси на маршрутизаторі, що має вихід до глобальної мережі:

R_0(config)#interface GigabitEthernet0/0
R_0(config-if)#ip address 175.0.1.1 255.255.255.252
R_0(config-if)#no shutdown
R_0(config-if)#exit

2. Налаштування статичної адреси на маршрутизаторі Linksys. Відкрийте вкладку Setup, та зі списку **Internet Connection type,** оберіть тип **StaticIP,** після чого налаштуйте IP-адресацію вручну. Приклад вкладки Setup з налаштованою статичною IP-адресацією наведено на рис. 2.5.

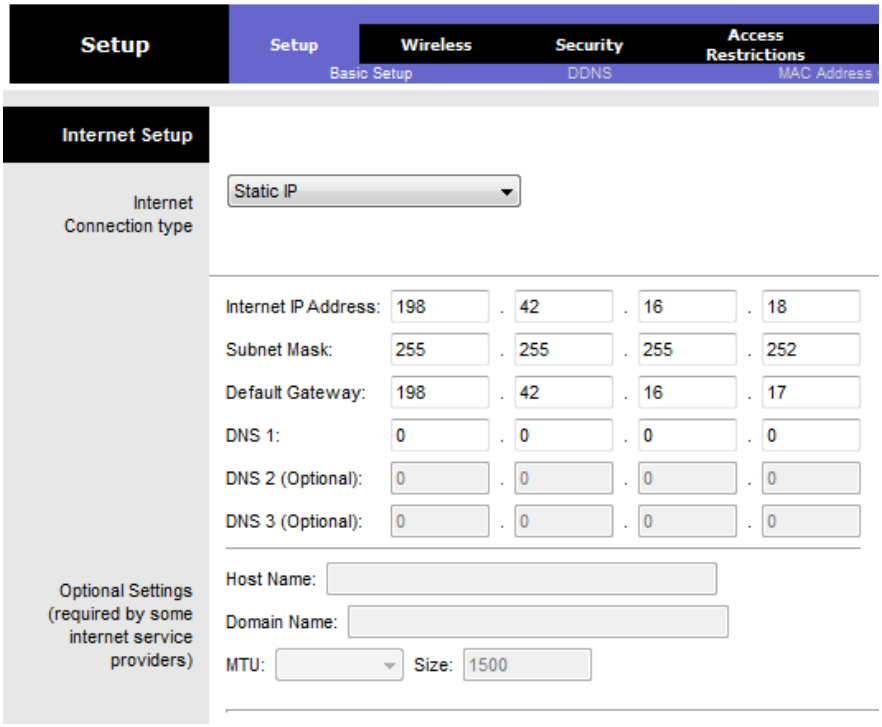

Рисунок 2.5 − Приклад налаштування статичної IP-адреси на маршрутизаторі Cisco Linksys WRT300N

3. Налаштування IP-адресації для локальної мережі маршрутизатора. Зазначається IP-адреса для майбутньої локальної мережі пристрою, максимальна кількість підключених користувачів (DHCP Pool), час оренди IP-адреси для користувача та статична адреса DNS (Рис. 2.6).

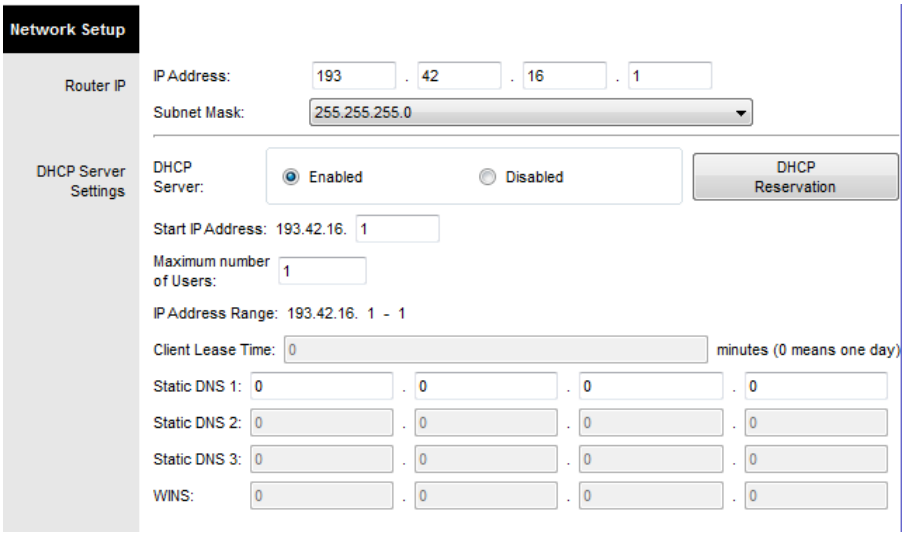

Рисунок 2.6 − Приклад налаштувань локальної мережі маршрутизатора

4. Вкладка Wireless дозволяє налаштувати бездротову точку доступу маршрутизатора. В рядку **Network Name (SSID)** змініть назву мережі на власну (Рис. 2.7).

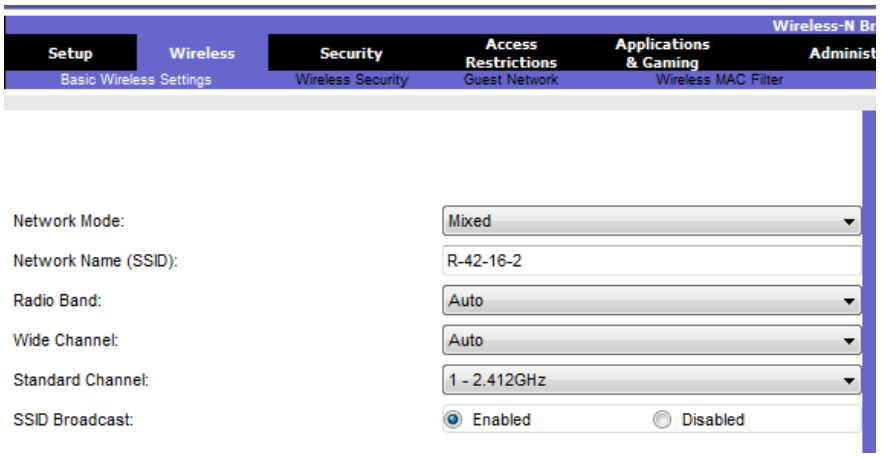

Рисунок 2.7 – Приклад налаштувань бездротової точки доступу маршрутизатора

5. Вкладка **Wireless Security** дозволяє обрати метод автентифікації. Встановіть **WEP** як метод автентифікації для параметру **Security Mode** (рис. 2.8)**.**

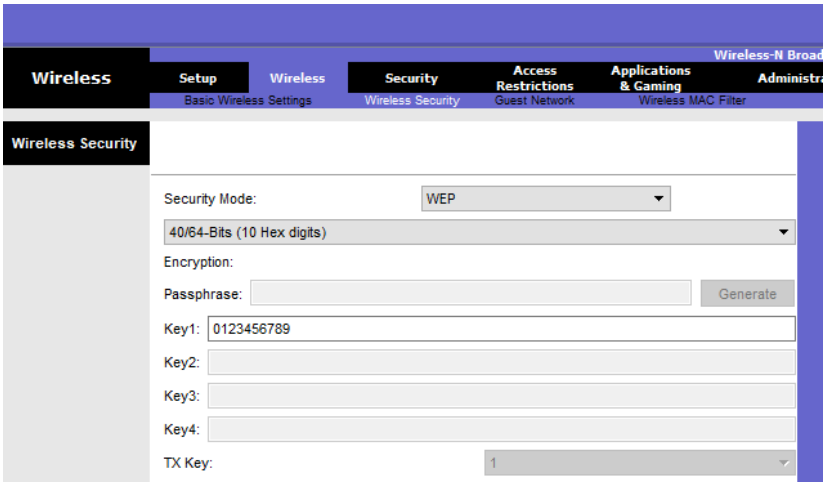

Рисунок 2.8 − Приклад налаштувань безпеки для точки доступу маршрутизатора

Модельний приклад налагодження маршрутизатора Linksys з динамічним отриманням адреси в Cisco Packet Tracer

Розглянемо специфіку налагодження мережі на базі маршрутизатора Linksys, схему якої наведено на рис. 2.9. Граничним маршрутизатором було обрано Cisco Router 2911.

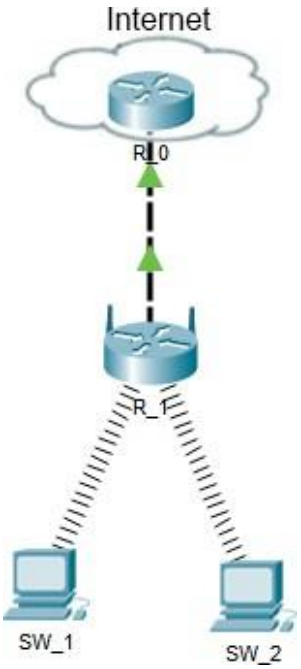

Рисунок 2.9 − Топологія мережі

Під час побудови мережі для з’єднання пристроїв використано дані табл. 6. Для налаштування параметрів адресації пристроїв використано дані табл. 7.

Таблиця 6

Параметри з'єднань пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R_1	Internet	Cloud	Gig0/0
	Wireless	Робоча станція WS_1	Wireless0
	Wireless	Робоча станція WS_2	Wireless0
Робоча станція WS_1	Wireless0	Маршрутизатор R_1	Wireless
Робоча станція WS_2	Wireless0	Маршрутизатор R_1	Wireless

Таблиця 7

Параметри адресації мереж для прикладу

Підмережа/ Пристрій	Інтерфейс/ Мережевий адаптер/ Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа A	-	175.0.1.0	255.255.255.252	/30
Підмережа B	-	192.168.0.0	255.255.255.0	/24
Маршрутизатор R_1	Internet	DHCP	-	-
	Wireless	192.168.0.1	255.255.255.0	/24
Робоча станція WS_1	Мережевий адаптер	192.168.0.2	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.0.1		
Робоча станція WS_2	Мережевий адаптер	192.168.0.2	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.0.1		

Сценарій налагодження маршрутизатора R_1 з динамічним отриманням адреси:

1. Налагодження DHCP на маршрутизаторі R_0

R_0(config)#interface GigabitEthernet0/0
R_0(config-if)#ip address 175.0.1.1 255.255.255.252
R_0(config-if)#no shutdown
R_0(config-if)#exit
R_0(config)#ip dhcp pool R_0-R_1
R_0(dhcp-config)#network 175.0.1.0 255.255.255.252
R_0(dhcp-config)#default-router 175.0.1.1
R_0(dhcp-config)#exit
R_0(config)#ip dhcp excluded-address 175.0.1.1

2. У вкладці **Setup,** зі списку **Internet Connection type,** обрати **Automatic Configuration – DHCP,** як показано на рис. 2.10.

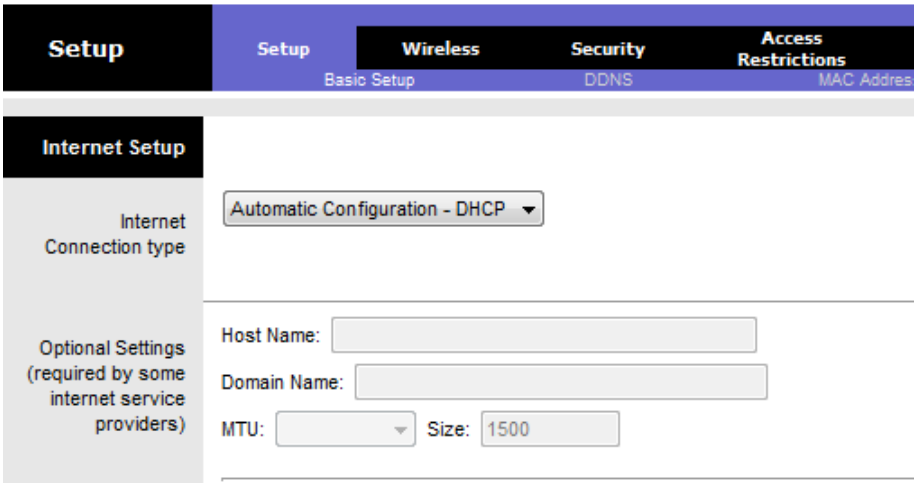

Рисунок 2.10 − Приклад налаштування з’єднання з автоматичним отриманням IP-адреси

3. Налаштування IP-адресації мережі аналогічне до попереднього сценарію (Рис. 2.11).

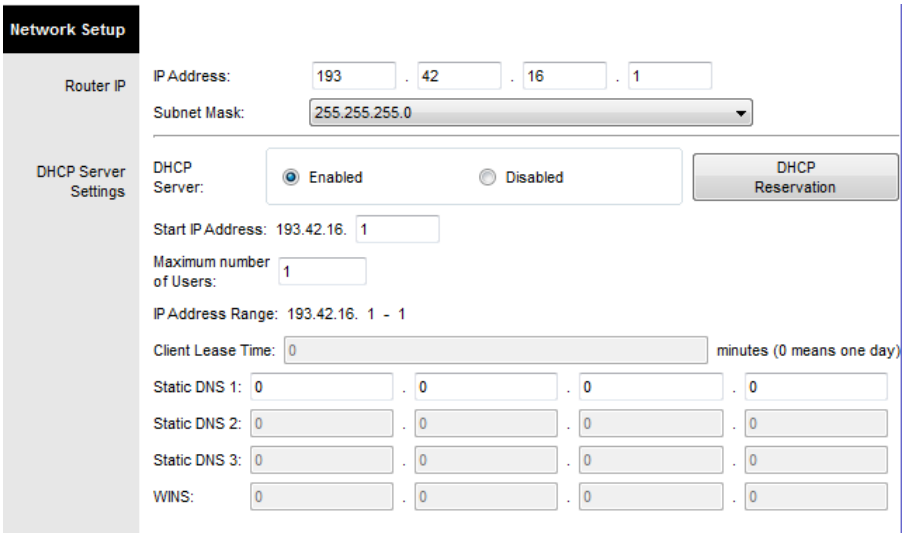

Рисунок 2.11 − Приклад налаштувань локальної мережі маршрутизатора

4. Вкладка Wireless дозволяє налаштувати бездротову точку доступу маршрутизатора. В рядку **Network Name (SSID)** змініть назву мережі на власну (Рис. 2.12).

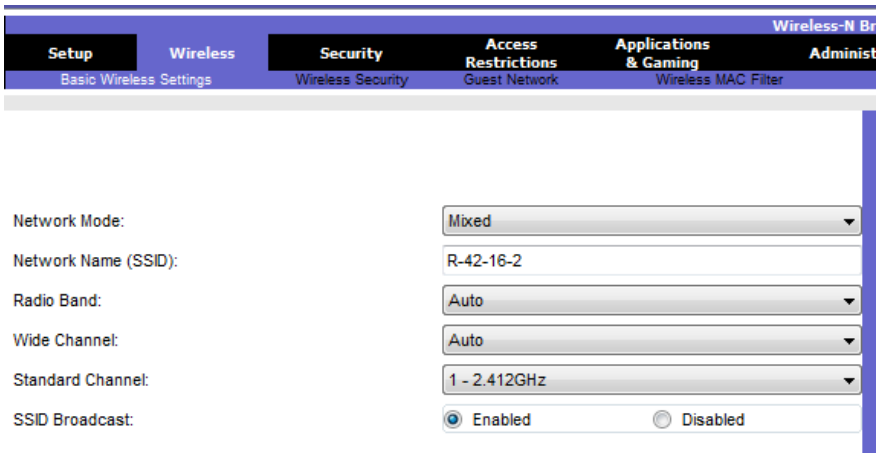

Рисунок 2.12 Приклад налаштувань бездротової точки доступу маршрутизатора

5. Змінимо метод автентифікації на **WPA-Personal**, як показано на рис. 2.13.

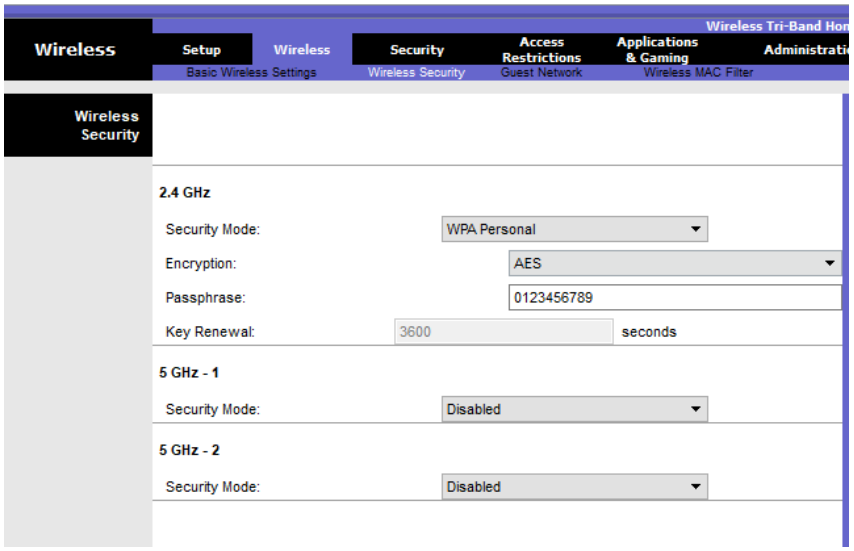

Рисунок 2.13 − Приклад налаштування безпеки для точки доступу маршрутизатора

Модельний приклад налагодження маршрутизатора Linksys з використанням протоколу PPPoE в Cisco Packet Tracer

Розглянемо специфіку налагодження мережі на базі маршрутизатора Linksys, схему якої наведено на рис. 2.14.

Граничним маршрутизатором було обрано Cisco Router 2911.

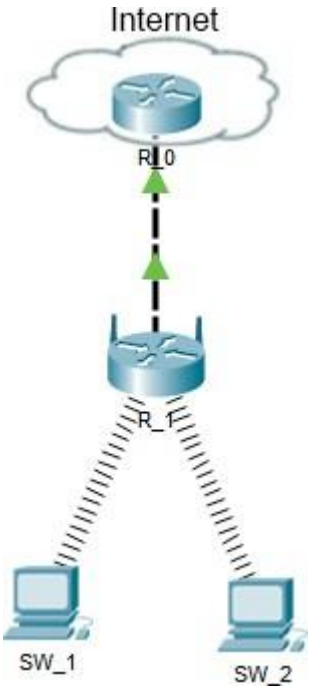

Рисунок 2.14 − Топологія мережі

Під час побудови мережі для з'єднання пристроїв використано дані табл. 8. Для налаштування параметрів адресації пристроїв використано дані табл. 9.

Таблиця 8

Параметри з'єднань пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R_1	Internet	Cloud	Gig0/0
	Wireless	Робоча станція WS_1	Wireless0
	Wireless	Робоча станція WS_2	Wireless0
Робоча станція WS_1	Wireless0	Маршрутизатор R_1	Wireless
Робоча станція WS_2	Wireless0	Маршрутизатор R_1	Wireless

Таблиця 9

Параметри адресації мереж для прикладу

Підмережа/ Пристрій	Інтерфейс/ Мережевий адаптер/ Шлюз	IP-адреса	Маска підмережі	Префікс
ПідмережаA	-	175.0.1.0	255.255.255.252	/30
ПідмережаB	-	192.168.0.0	255.255.255.0	/24
Маршрутизатор R_1	Internet	PPPoE	-	-
	Wireless	192.168.0.1	255.255.255.0	/24
Робоча станція WS_1	Мережевий адаптер	192.168.0.2	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.0.1		
Робоча станція WS_2	Мережевий адаптер	192.168.0.2	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.0.1		

1. Налагодження маршрутизатора R_4 з PPPoE підключенням до інтернету.

R_0(config)#interface GigabitEthernet0/0
R_0(config-if)#ip address 175.0.1.1 255.255.255.252
R_0(config-if)#no shut
R_0(config-if)#exit
R_0(config)#username R_1 password R_1
R_0(config)#bba-group pppoe Router
R_0(config-bba)#
R_0(config-bba)#virtual-template 1
R_0(config-bba)#interface Virtual-Template1
R_0(config-if)#peer default ip address pool Router
R_0(config-if)#ppp authentication chap callin
R_0(config-if)#ip unnumbered GigabitEthernet0/0
R_0(config-if)#exit
R_0(config)#interface GigabitEthernet 0/0
R_0(config-if)#pppoe enable group Router
R_0(config-if)#exit
R_0(config)#ip local pool Router 175.0.1.2 175.0.1.2
R_0(config)#

2. У вкладці **Setup** зі списку **Internet Connection type,** необхідно обрати **PPPoE** (рис. 2.15). Після чого ввести ім’я користувача та пароль, які були використані при налаштуванні PPoE на маршрутизаторі **R_1**. Поле **Service Name** є опціональним, його варто залишити порожнім.

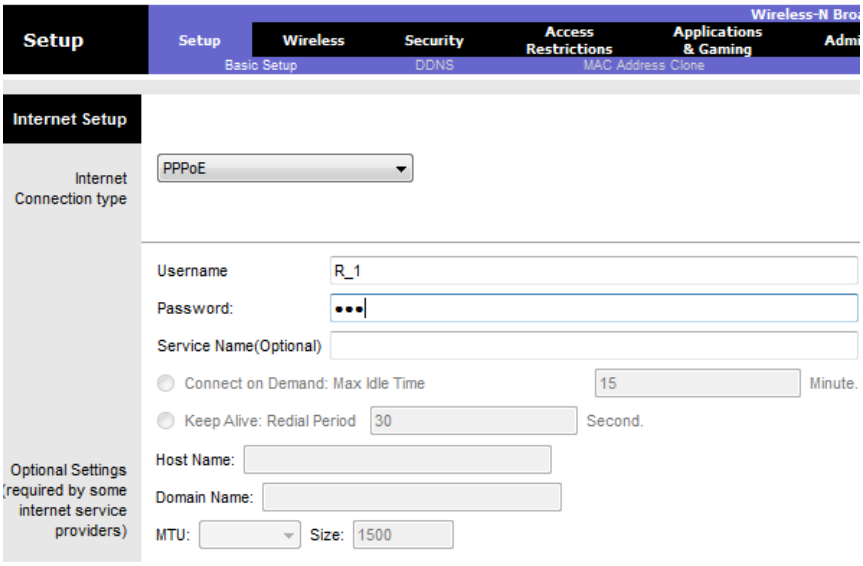

Рисунок 2.15 − Приклад налаштування підключення з використанням PPPoE

3. Налаштування IP-адресації в локальній мережі аналогічне до попереднього сценарію (рис. 2.16).

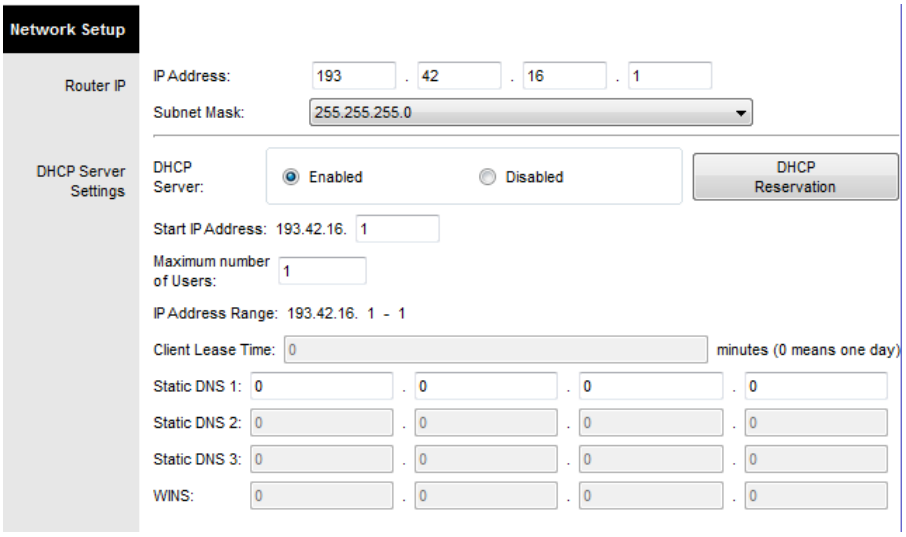

Рисунок 2.16 − Приклад налаштувань локальної мережі маршрутизатора

4. Вкладка Wireless дозволяє налаштувати бездротову точку доступу маршрутизатора. В рядку **Network Name (SSID)** змініть назву мережі на власну (Рис. 2.17).

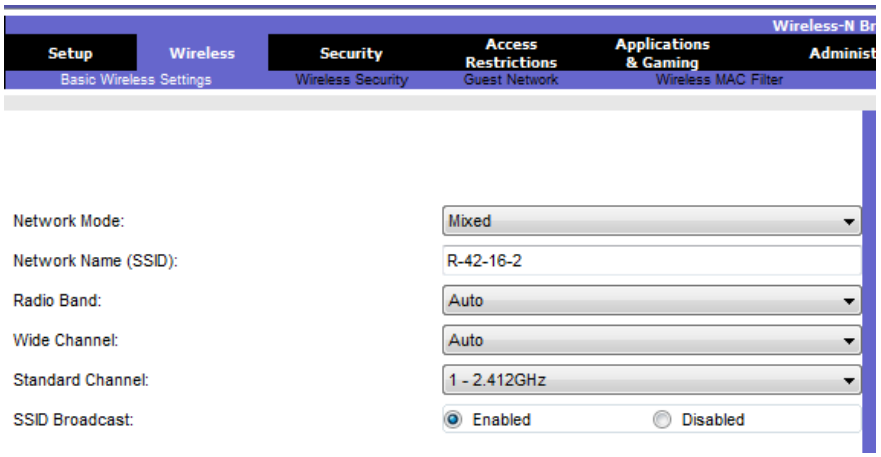

Рисунок 2.17 – Приклад налаштувань бездротової точки доступу маршрутизатора

5. Змінимо метод автентифікації на **WPA-Personal**, як показано на рис. 2.18.

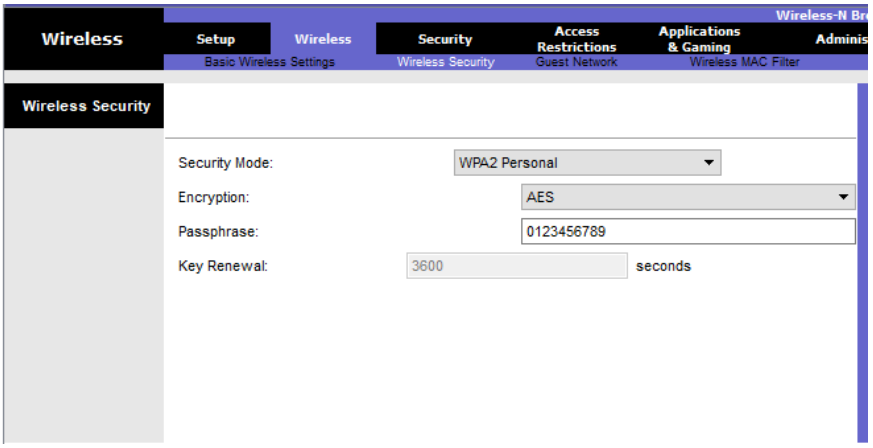

Рисунок 2.18 – Приклад налаштування режиму безпеки для точки доступу маршрутизатора

Завдання на лабораторну роботу

1. У середовищі програмного симулятора/емулятора створити проєкт мережі (рис. 2.19). Для побудованої мережі заповнити описову таблицю, яка аналогічна табл. 4.

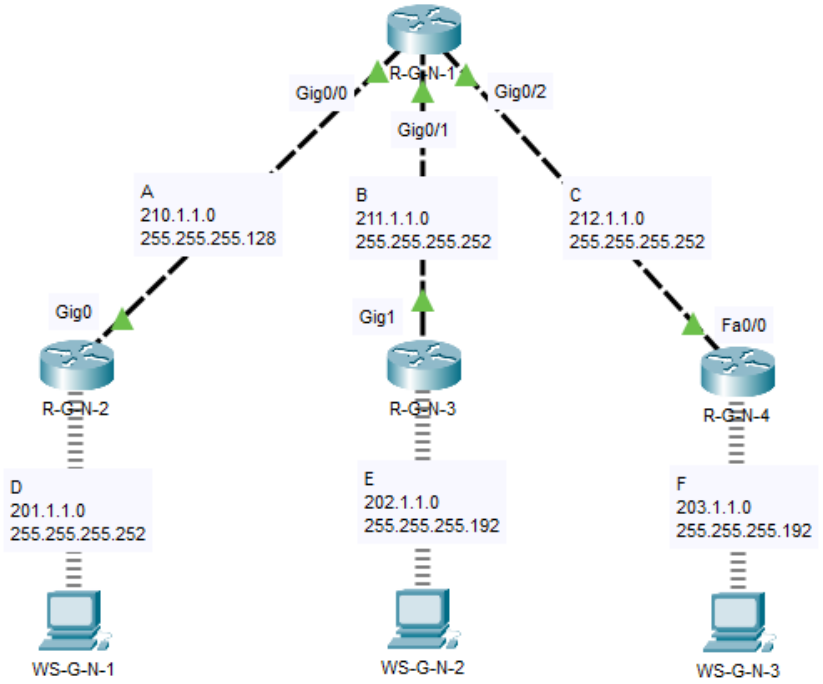

Рисунок 2.19 − Проєкт мережі

2. Розробити схему адресації пристроїв мережі. Для цього використовувати дані табл. 10. Результати навести у вигляді таблиці, яка аналогічна табл. 5.

3. Провести базове налагодження пристроїв, інтерфейсів та каналів зв’язку. Провести налагодження параметрів IP-адресації пристроїв мережі відповідно до даних, які отримані у п. 2. Перевірити наявність зв’язку між сусідніми парами пристроїв мережі.

4. Провести налагодження підключення між маршрутизаторами мережі. Для вибору методу та протоколу використовувати дані табл. 11. Перевірити зв’язок між пристроями.

5. Налагодити Wi-Fi мережі між маршрутизаторами та робочими станціями. Скористатися даними табл. 12. Для назви мережі використовувати формат W_G_N_X, де G-номер групи, а N-номер варіанта.

Таблиця 10

Адресація пристроїв мережі

№ варіанта	Підмережа А		Підмережа В		Підмережа С	
	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс
1	196.G.N.0	/30	197.G.N.0	/30	198.G.N.8	/30
2	196.G.N.4	/30	197.G.N.20	/30	198.G.N.28	/30
3	196.G.N.8	/30	197.G.N.40	/30	198.G.N.48	/30
4	196.G.N.12	/30	197.G.N.60	/30	198.G.N.68	/30
5	196.G.N.16	/30	197.G.N.80	/30	198.G.N.88	/30
6	196.G.N.20	/30	197.G.N.4	/30	198.G.N.12	/30
7	196.G.N.24	/30	197.G.N.24	/30	198.G.N.32	/30
8	196.G.N.28	/30	197.G.N.44	/30	198.G.N.52	/30
9	196.G.N.32	/30	197.G.N.64	/30	198.G.N.72	/30
10	196.G.N.36	/30	197.G.N.84	/30	198.G.N.92	/30
11	196.G.N.40	/30	197.G.N.8	/30	198.G.N.16	/30
12	196.G.N.44	/30	197.G.N.28	/30	198.G.N.36	/30
13	196.G.N.48	/30	197.G.N.48	/30	198.G.N.56	/30
14	196.G.N.52	/30	197.G.N.68	/30	198.G.N.76	/30
15	196.G.N.56	/30	197.G.N.88	/30	198.G.N.96	/30
16	196.G.N.60	/30	197.G.N.12	/30	198.G.N.16	/30
17	196.G.N.64	/30	197.G.N.32	/30	198.G.N.36	/30
18	196.G.N.68	/30	197.G.N.52	/30	198.G.N.56	/30
19	196.G.N.72	/30	197.G.N.72	/30	198.G.N.76	/30
20	196.G.N.76	/30	197.G.N.92	/30	198.G.N.96	/30
21	196.G.N.80	/30	197.G.N.16	/30	198.G.N.0	/30
22	196.G.N.84	/30	197.G.N.36	/30	198.G.N.20	/30
23	196.G.N.88	/30	197.G.N.56	/30	198.G.N.40	/30
24	196.G.N.92	/30	197.G.N.76	/30	198.G.N.60	/30
25	196.G.N.96	/30	197.G.N.96	/30	198.G.N.80	/30
26	196.G.N.4	/30	197.G.N.16	/30	198.G.N.4	/30
27	196.G.N.24	/30	197.G.N.36	/30	198.G.N.24	/30
28	196.G.N.44	/30	197.G.N.56	/30	198.G.N.44	/30
29	196.G.N.64	/30	197.G.N.76	/30	198.G.N.64	/30
30	196.G.N.84	/30	197.G.N.96	/30	198.G.N.84	/30

Продовження табл. 10

№ варіанта	Підмережа D		Підмережа E		Підмережа F	
	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс
1	193.G.N.0	/25	193.G.N.128	/25	200.G.N.0	/24
2	193.G.N.0	/26	193.G.N.64	/26	200.G.N.0	/25
3	193.G.N.128	/26	193.G.N.192	/26	200.G.N.0	/26
4	193.G.N.0	/27	193.G.N.32	/27	200.G.N.0	/27
5	193.G.N.64	/27	193.G.N.96	/27	200.G.N.0	/28
6	193.G.N.128	/27	193.G.N.160	/27	200.G.N.0	/24
7	193.G.N.192	/27	193.G.N.224	/27	200.G.N.0	/25
8	193.G.N.0	/28	193.G.N.16	/28	200.G.N.0	/26
9	193.G.N.32	/28	193.G.N.48	/28	200.G.N.0	/27
10	193.G.N.64	/28	193.G.N.80	/28	200.G.N.0	/28
11	193.G.N.96	/28	193.G.N.112	/28	200.G.N.0	/24
12	193.G.N.128	/28	193.G.N.144	/28	200.G.N.0	/25
13	193.G.N.160	/28	193.G.N.176	/28	200.G.N.0	/26
14	193.G.N.192	/28	193.G.N.208	/28	200.G.N.0	/27
15	193.G.N.224	/28	193.G.N.240	/28	200.G.N.0	/28
16	193.G.N.0	/25	193.G.N.128	/25	200.G.N.0	/24
17	193.G.N.0	/26	193.G.N.64	/26	200.G.N.0	/25
18	193.G.N.128	/26	193.G.N.192	/26	200.G.N.0	/26
19	193.G.N.0	/27	193.G.N.32	/27	200.G.N.0	/27
20	193.G.N.64	/27	193.G.N.96	/27	200.G.N.0	/28
21	193.G.N.128	/27	193.G.N.160	/27	200.G.N.0	/24
22	193.G.N.192	/27	193.G.N.224	/27	200.G.N.0	/25
23	193.G.N.0	/28	193.G.N.16	/28	200.G.N.0	/26
24	193.G.N.32	/28	193.G.N.48	/28	200.G.N.0	/27
25	193.G.N.64	/28	193.G.N.80	/28	200.G.N.0	/28
26	193.G.N.96	/28	193.G.N.112	/28	200.G.N.0	/24
27	193.G.N.128	/28	193.G.N.144	/28	200.G.N.0	/25
28	193.G.N.160	/28	193.G.N.176	/28	200.G.N.0	/26
29	193.G.N.192	/28	193.G.N.208	/28	200.G.N.0	/27
30	193.G.N.224	/28	193.G.N.240	/28	200.G.N.0	/28

Таблиця 11

Дані для маршрутизації

№ Варіанта	Маршрутизатори		
	R_G_N_2	R_G_N_3	R_G_N_4
1	Static	PPPoE	DHCP
2	Static	DHCP	PPPoE
3	PPPoE	Static	DHCP
4	PPPoE	DHCP	Static
5	DHCP	PPPoE	Static
6	DHCP	Static	PPPoE
7	Static	PPPoE	DHCP
8	Static	DHCP	PPPoE
9	PPPoE	Static	DHCP
10	PPPoE	DHCP	Static
11	DHCP	PPPoE	Static
12	DHCP	Static	PPPoE
13	Static	PPPoE	DHCP
14	Static	DHCP	PPPoE
15	PPPoE	Static	DHCP
16	PPPoE	DHCP	Static
17	DHCP	PPPoE	Static
18	DHCP	Static	PPPoE
19	Static	PPPoE	DHCP
20	Static	DHCP	PPPoE
21	PPPoE	Static	DHCP
22	PPPoE	DHCP	Static
23	DHCP	PPPoE	Static
24	DHCP	Static	PPPoE
25	Static	PPPoE	DHCP
26	Static	DHCP	PPPoE
27	PPPoE	Static	DHCP
28	PPPoE	DHCP	Static
29	DHCP	PPPoE	Static
30	DHCP	Static	PPPoE

Таблиця 12

Механізм адресації кінцевих вузлів локальних мереж

№ варіанта	Мережа		
	D	E	F
1	Static	DHCP	DHCP
2	DHCP	Static	DHCP
3	DHCP	DHCP	Static
4	Static	DHCP	DHCP
5	DHCP	Static	DHCP
6	DHCP	DHCP	Static
7	Static	DHCP	DHCP
8	DHCP	Static	DHCP
9	DHCP	DHCP	Static
10	Static	DHCP	DHCP
11	DHCP	Static	DHCP
12	DHCP	DHCP	Static
13	Static	DHCP	DHCP
14	DHCP	Static	DHCP
15	DHCP	DHCP	Static
16	Static	DHCP	DHCP
17	DHCP	Static	DHCP
18	DHCP	DHCP	Static
19	Static	DHCP	DHCP
20	DHCP	Static	DHCP
21	DHCP	DHCP	Static
22	Static	DHCP	DHCP
23	DHCP	Static	DHCP
24	DHCP	DHCP	Static
25	Static	DHCP	DHCP
26	DHCP	Static	DHCP
27	DHCP	DHCP	Static
28	Static	DHCP	DHCP
29	DHCP	Static	DHCP
30	DHCP	DHCP	Static

Контрольні запитання

1. Рекомендації з підвищення рівня захищеності бездротової мережі на маршрутизаторах Cisco Linksys.
2. Загальна характеристика маршрутизатора Cisco Linksys WRT300N.
3. Наведіть перелік та поясніть призначення основних команд для налагодження бездротової мережі на маршрутизаторах Cisco Linksys.
4. Загальні відомості про фірму Linksys.
5. Основні команди налагодження маршрутизатора Linksys з статичним типом з'єднання з Інтернетом.
6. Основні команди налагодження маршрутизатора Linksys з використанням протоколу PPPoE.
7. Основні команди налагодження маршрутизатора Linksys з динамічним отриманням адреси.
8. Наведіть перелік та поясніть призначення графічних засобів налагодження бездротової мережі на маршрутизаторах Linksys.
9. Наведіть перелік протоколів безпеки, які можна налаштувати на маршрутизаторі Linksys.
10. Назвіть можливі варіанти первинного налаштування маршрутизатора Linksys.
11. Наведіть підтримувані стандарти бездротових локальних мереж.
12. Які протоколи дистанційного керування підтримуються маршрутизатором.
13. Назвіть мережеві/транспортні протоколи, що підтримуються маршрутизатором.
14. Алгоритми шифрування на маршрутизаторах Linksys.
15. Які технології підключення підтримуються маршрутизатором Linksys.
16. Протоколи дистанційного керування.

Лабораторна робота № 3: Налагодження та дослідження роботи бездротових мереж, побудованих на базі маршрутизаторів Cisco

Мета роботи: ознайомитися з можливостями маршрутизаторів Cisco для побудови бездротових мереж Wi-Fi; розглянути засоби організації мережевих з'єднань між пристроями Wi-Fi мережі; ознайомитися з можливостями мережевої операційної системи Cisco IOS стосовно налагодження бездротових з'єднань; отримати практичні навички налагодження, моніторингу та діагностування роботи бездротової мережі, побудованої на базі маршрутизаторів Cisco; дослідити процеси роботи маршрутизаторів Cisco та процеси передачі даних у побудованій мережі Wi-Fi.

Теоретичні відомості

У сучасному світі бездротові мережі стали невід'ємною частиною нашого повсякденного життя, забезпечуючи зручний доступ до інформаційних ресурсів у будь-якому місці та в будь-який час. Вони дозволяють користувачам підключатися до Інтернету та локальних мереж без необхідності фізичних з'єднань, що істотно підвищує мобільність і гнучкість. Бездротові технології, такі як Wi-Fi, використовують радіохвилі для передачі даних, що робить їх ідеальними для використання в домашніх, офісних та публічних середовищах. Оскільки потреби в бездротовому з'єднанні постійно зростають, належне налагодження та моніторинг таких мереж стають критично важливими для забезпечення стабільності, безпеки та високої продуктивності.

Обладнання для створення професійних бездротових мереж є перспективним для ІТ-компаній, і на сьогоднішній день список цих компаній зростає. Основними компонентами бездротової мережі є:

- Wi-Fi контроллер точки доступу (Access Point Controller);
- Wi-Fi точка доступу (Access Point);
- Wi-Fi антени точок доступу;
- маршрутизатор (Router);
- комутатор (Switch);
- адаптери, модулі та ін.

Wi-Fi контроллер — це пристрій або програмне забезпечення, яке централізовано керує однією або декількома точками доступу в бездротовій мережі. Він відповідає за налаштування, моніторинг, управління трафіком та забезпечення безпеки, дозволяючи адміністраторам легко налаштовувати мережу без потреби в конфігурації кожної точки доступу окремо.

Wi-Fi точка доступу (Wireless Access Point, WAP) — дозволяє бездротовим клієнтам підключатися до хмарної мережі (дротової або бездротової). Вона виступає як міст між бездротовими пристроями та локальною мережею, забезпечуючи з'єднання, передачу даних та доступ до Інтернету.

Wi-Fi антени точок доступу — компоненти, які використовуються для покращення бездротового сигналу. Вони можуть бути вбудованими або зовнішніми, і їхнє призначення полягає в підвищенні дальності, потужності та якості сигналу, що передається між точкою доступу та підключеними пристроями.

Маршрутизатори Wi-Fi дозволяють швидко та легко встановлювати зв’язок в загальнодоступній мережі Інтернет для дротової або бездротової мережі. Wi-Fi бездротовий маршрутизатор (роутер), а також дротові маршрутизатори призначені передачі трафіку в мережі. Маршрутизатор Wi-Fi має одну або дві антени для роботи з мережею Wi-Fi та локальним мережевим кабелем для підключення всередині мережі користувачів та мережі, що підключає зовнішній канал зв'язку.

Таким чином, маршрутизатор Wi-Fi об'єднує дротові мережі та мережі Wi-Fi. Всі маршрутизатори Wi-Fi управляються через веб-інтерфейс. Захист інформації, що передається через Wi-Fi, забезпечують протоколи WPA/WPA2-RADIUS, WPA/WPA2-PSK та WEP. Фільтр MAC-адрес виключає несанкціоноване підключення до мережі.

Комутатори служать для підключення точок та контролерів однієї мережі та забезпечують можливість передачі живлення та інформації на відстані до 100 м через один кабель (вита пара) за технологією Ethernet (PoE).

Адаптери, модулі та інші подібні компоненти — дозволяють підключати різні види мережевих інтерфейсів до комп’ютерів, маршрутизаторів або інших пристроїв. Наприклад, Wi-Fi адаптер може перетворювати дротове з’єднання в бездротове, а мережеві модулі можуть додавати специфічні функції чи покращувати продуктивність мережі. Wi-Fi PCI-адаптер вважається одним із найпоширеніших (рис. 3.1).

Рисунок 3.1 − Wi-Fi PCI-адаптер

Стандарти захисту мереж Wi-Fi

Зростання використання Wi-Fi супроводжується і підвищеним ризиком безпеки, оскільки відкрите повітряне середовище передбачає можливість несанкціонованого доступу до мережі. Тому стандарти захисту мереж Wi-Fi набувають особливої ваги, адже вони визначають принципи шифрування, автентифікації та контролю доступу. Від старих стандартів, таких як WEP, до сучасних протоколів WPA2 та WPA3, ці технології розвиваються з метою забезпечення надійного захисту даних, що передаються в бездротових мережах, та підтримки конфіденційності користувачів.

WEP

Протокол шифрування, що використовує досить не стійкий алгоритм RC4 на статичному ключі. Існує 64, 128, 256 і 512-бітове WEP шифрування. Чим більше біт використовується для зберігання ключа, тим більше можливих комбінацій ключів, а відповідно більш висока стійкість мережі до злому. Частина WEP ключа є статичною (40 біт в разі 64-бітного шифрування) а інша частина (24 біт) – динамічна (вектор ініціалізації), тобто змінюється в процесі роботи мережі. Основною вразливістю протоколу WEP є те, що вектори ініціалізації повторюються через деякий проміжок часу і зловмиснику буде потрібно лише зібрати ці повтори і обчислити по ним статичну частину ключа. Для підвищення рівня безпеки можна додатково до WEP шифрування використовувати стандарт 802.1x або VPN.

WPA

Більш стійкий протокол шифрування, ніж WEP, хоча використовується такий же алгоритм RC4. Більш високий рівень безпеки досягається за рахунок використання протоколів TKIP і MIC.

- *TKIP (Temporal Key Integrity Protocol). Протокол динамічних ключів мережі, які змінюються досить часто. При цьому кожному пристрою також присвоюється ключ, який теж змінюється.*
- *MIC (Message Integrity Check). Протокол перевірки цілісності пакетів. Захищає від перехоплення пакетів та перенаправлення.*

Також можливе і використання 802.1x і VPN, як і в випадку з WEP.

Існує два види WPA:

- *WPA-PSK (Pre-shared key). Для генерації ключів мережі і для входу в мережу використовується ключова фраза. Оптимальний варіант для домашньої або невеликої офісної мережі.*

- *WPA-802.1x. Вхід в мережу здійснюється через сервер аутентифікації. Оптимально для мережі великої компанії.*

WPA2

Удосконалення протоколу WPA. На відміну від WPA, використовується більш стійкий алгоритм шифрування AES. Аналогічно з WPA, WPA2 ділиться на два типи: WPA2-PSK та WPA2-802.1x.

WPA3

Wi-Fi Protected Access 3 (WPA3) - вдосконалення існуючих можливостей безпеки WPA2 для 802.11. Він підтримує нові методи безпеки, забороняє використання застарілих протоколів та вимагає використання захисту кадрів керування (MFP) для підтримки стійкості критично важливих мереж. WPA3 також ділиться на два типи: WPA3-Personal та WPA3-Enterprise.

WPA3-Personal використовує одночасну автентифікацію рівних (SAE), що замінило собою вразливий до атак PSK, щоб захистити користувачів від атак із підбіром пароля. WPA3-Enterprise пропонує додатковий еквівалент 192-бітної надійності шифрування.

802.1X

Стандарт безпеки, в який входить кілька протоколів:

- *EAP (Extensible Authentication Protocol). Протокол розширеної аутентифікації. Використовується спільно з RADIUS сервером у великих мережах.*
- *TLS (Transport Layer Security). Протокол, який забезпечує цілісність і шифрування переданих даних між сервером і клієнтом, їх взаємну аутентифікацію, запобігаючи перехопленню та підміні повідомлень.*
- *RADIUS (Remote Authentication Dial-In User Server). Віддалений сервер аутентифікації користувачів за логіном і паролем.*

Enhanced Open

Enhanced Open визначає покращену конфіденційність даних у відкритих мережах Wi-Fi. Ця сертифікація базується на протоколі Opportunistic Wireless Encryption (OWE). OWE визначено в IETF RFC 8110. Протокол OWE інтегрує встановлені механізми криптографії, щоб надати кожному користувачеві унікальне індивідуальне шифрування, захищаючи обмін даними між користувачем і точкою доступу. Взаємодія з користувачем така ж, як і з відкритою безпекою, оскільки немає необхідності вводити пароль або парольну фразу перед приєднанням до мережі. Зловмисні атаки підслуховування пом’якшуються, оскільки кадри даних 802.11 зашифровані, але автентифікація відсутня. Enhanced Open не є частиною WPA3 і є зовсім іншою та додатковою сертифікацією безпеки. Існує два режими роботи OWE: Enhanced Open Only, Enhanced Open Transition.

Огляд можливостей бездротових маршрутизаторів Cisco

Бездротові маршрутизатори Cisco відомі своєю надійністю, потужністю та широким спектром функцій, які задовольняють потреби як домашнього, так і корпоративного сегментів. Вони підтримують різноманітні бездротові стандарти, включаючи останні версії Wi-Fi 5 та Wi-Fi 6, що забезпечує високу швидкість передачі даних та поліпшену продуктивність у середовищах з великою кількістю підключених пристроїв. Cisco також пропонує розширені можливості безпеки, такі як вбудовані фільтри вмісту, контроль доступу та підтримка протоколів WPA3, що дозволяє забезпечити захист від несанкціонованого доступу. Крім того, маршрутизатори Cisco оснащені функціями для управління мережею, такими як Cisco DNA, що забезпечує моніторинг та аналітику в реальному часі. Завдяки своїй гнучкості та масштабованості, бездротові маршрутизатори Cisco ідеально підходять для створення як малих, так і великих мереж, здатних адаптуватися до змінюваних вимог користувачів.

Якщо вести мову про бездротові маршрутизатори Cisco, то варто розуміти, що ці пристрої в першу чергу орієнтовані на побудову мереж типу SOHO.

Найбільш відомими серіями таких маршрутизаторів є: Aironet, Catalyst, Linksys, Meraki, ISR та 8800.

Характеристики основних бездротових маршрутизаторів із вбудованими бездротовими модулями наведені у табл. 1.

Таблиця 1

Основні характеристики бездротових маршрутизаторів

Маршрутизатор	829	1800	Linksys WRT54GL
Серія	Cisco 800 Series	Cisco IR1835 Series	Linksys
WAN порти Ethernet	1 x 4G	1 x GE+SFP, 2 x 4G	1 x FE
LAN порти Ethernet	4 x FE	4 x GE	4 x FE
Пам’ять FLASH	4 Гб	4 Гб	–
Об’єм ОЗП	2 Гб	8 Гб	–
Потужність номінальна / максимальна	40 Ват	22-23 Ват / 27 Ват, 71 Ват (PoE)	40 Ват
Тип живлення	PoE	AC 100-240В / PoE	AC 100-240В
Тип установки	Настільний	Настільний	Настільний
Порти консольні	RJ-45 (RS232)	RJ-45 (RS232, RS485)	–
Порти USB	1 x Mini-USB	1 x Mini-USB, 1 x USB	–
Антени	–	2 зовнішніх 2.4 GHz 2xRP-TNC / 5 GHz 2xRP-TNC, 1 x GPS	2 зовнішніх

Окрім зазначених серій, компанія Cisco також розробила бездротові рішення для обладнання, яке не підтримувало даний функціонал, зокрема завдяки спеціальним модулям розширення. Прикладом розширення функціоналу може слугувати встановлення такого модуля в маршрутизатор моделі Cisco 2811.

Основні моделі бездротових модулів стандартів Wi-Fi наведені нижче:

- Cisco HWIC-AP-AG-N – модуль компанії Cisco, призначений для надання бездротового доступу всередині приміщення. Простий у застосуванні, модуль вбудовується в різні серії маршрутизаторів Cisco (рис. 3.2).

Рисунок 3.2 – Зовнішній вигляд модуля Cisco HWIC-AP-AG-N

Як можна побачити вище, модуль включає в себе два коаксіальних порта для підключення двох змінних антен, а також здатний працювати в стандартах бездротової передачі даних 802.11a, 802.11b і 802.11g. Тобто, модуль має дводіапазонну частотну підтримку - 2,4 і 5 ГГц. Стандарт 802.11a призначений для роботи в верхньому частотному діапазоні (5 ГГц), а стандарти 802.11b і 802.11g працюють в нижньому частотному діапазоні (2,4 ГГц). Максимальна швидкість передачі даних складає 54 Мбіт / с для стандартів 802.11a і 802.11g, та 11 Мбіт / с для стандарту 802.11b.

Однак швидкість передачі при віддаленні взаємодіючих пристроїв один від одного поступово падає. Так, на відкритому повітрі при швидкості 1 Мбіт / с максимальна дальність зв'язку може досягати 600 м, а при швидкості 54 Мбіт / с - не більше 90 м.

Характерним є те, що модуль Cisco HWIC-AP-AG-N призначений для використання в стандартному настільному маршрутизаторі. Маршрутизатори не підтримують одночасну роботу двох і більше модулів.

Модуль Cisco HWIC-AP-AG-N підтримує всі сучасні методи безпечної передачі даних. До них відносяться: підтримка алгоритмів шифрування даних WEP, WPA і WPA2 з ключем до 128 біт, використання алгоритмів AES і TKIP та інші стандартні методи. У побудованій на основі модуля Cisco HWIC-AP-AG-N мережі можливо використовувати до 16 зашифрованих або незашифрованих віртуальних мереж VLAN.

Наразі існують наступні модифікації модуля:

- Cisco HWIC-AP-AG-E – двоканальний модуль, який підтримує стандарти 802.11 a/b/g в діапазонах 2.4 ГГц та 5 ГГц, призначений для використання у Європі.
- Cisco HWIC-AP-G-A – модуль, який підтримує стандарти 802.11 b/g, призначений для використання у Америці.
- Cisco HWIC-AP-G-B – модуль, який підтримує стандарти 802.11 a/b/g, призначений для використання у Америці.
- Cisco HWIC-AP-G-J – модуль, який підтримує стандарти 802.11 b/g, призначений для використання у Японії.
- Cisco HWIC-AP-AG-P – модуль, який підтримує стандарти 802.11 a/b/g, призначений для використання у Америці.

Команди Cisco IOS для налагодження бездротових каналів зв'язку стандарту 802.11 для маршрутизаторів Cisco

service-module wlan-ap 0 session – вхід до сервісного режиму налагодження точки доступу;

dot11 SSID [назва мережі] – налагодження точки доступу;

authentication open – налагодження відкритої точки доступу;

authentication key-management wpa– налагодження методу аутентифікації WPA;

wpa-psk ascii 0 [пароль] – налагодження захищеного доступу до Wi-Fi за допомогою WPA-PSK;

encryption mode ciphers aes-ccm – налагодження алгоритму шифрування WPA AES;

encryption mode ciphers tkip – налагодження алгоритму шифрування WPA TKIP;

encryption mode ciphers wep128 – налагодження алгоритму шифрування WEP, довжина ключа 128 біт;

encryption mode ciphers wep40 – налагодження алгоритму шифрування WEP, довжина ключа 40 біт;

Порядок налагодження бездротового каналу зв'язку стандарту 802.11 для маршрутизатора Cisco 819

Налагодження бездротового каналу зв'язку стандарту 802.11 для маршрутизатора Cisco 819 складається із певних етапів. Порядок виконання згаданих етапів є таким:

1. Увійти до сервісного режиму налагодження точки доступу.
2. Увійти у привілейований режим.
3. Увійти у режим конфігурування терміналу.
4. Налагодити ім'я точки доступу.
5. Налагодити метод аутентифікації.
6. Налагодити бездротовий інтерфейс точки доступу.

Порядок налагодження бездротового каналу зв'язку стандарту 802.11 для маршрутизатора Cisco 829

Налагодження бездротового каналу зв'язку стандарту 802.11 для маршрутизатора Cisco 829 складається із певних етапів. Порядок виконання згаданих етапів є таким:

1. Увійти у привілейований режим.
2. Увійти у режим конфігурування терміналу.
3. Налагодити IP-адресацію на бездротовому інтерфейсі.
4. Вийти у привілейований режим.
5. Увійти до сервісного режиму налагодження точки доступу.
6. Увійти в привілейований режим.
7. Увійти в режим конфігурування терміналу.
8. Налагодити ім'я точки доступу.
9. Налагодити метод аутентифікації.
10. Налагодити бездротовий інтерфейс точки доступу.

Порядок налагодження бездротового каналу зв'язку стандарту 802.11 для маршрутизатора Cisco 2811 з модулем HWIC-AP-AG-B

Налагодження бездротового каналу зв'язку стандарту 802.11 для маршрутизатора Cisco 2811 з модулем HWIC-AP-AG-B складається із певних етапів. Порядок виконання згаданих етапів є таким:

1. Увійти у привілейований режим.
2. Увійти у режим конфігурування терміналу.
3. Налагодити ім'я точки доступу.
4. Налагодити метод аутентифікації.
5. Налагодити бездротовий інтерфейс точки доступу.

Модельний приклад налагодження функціонування бездротової комп'ютерної мережі на базі маршрутизатора Cisco 819HGW

Розглянемо специфіку налагодження бездротових параметрів функціонування маршрутизатора Cisco моделі HGW819. Результат такого підключення наведений на рис. 3.3.

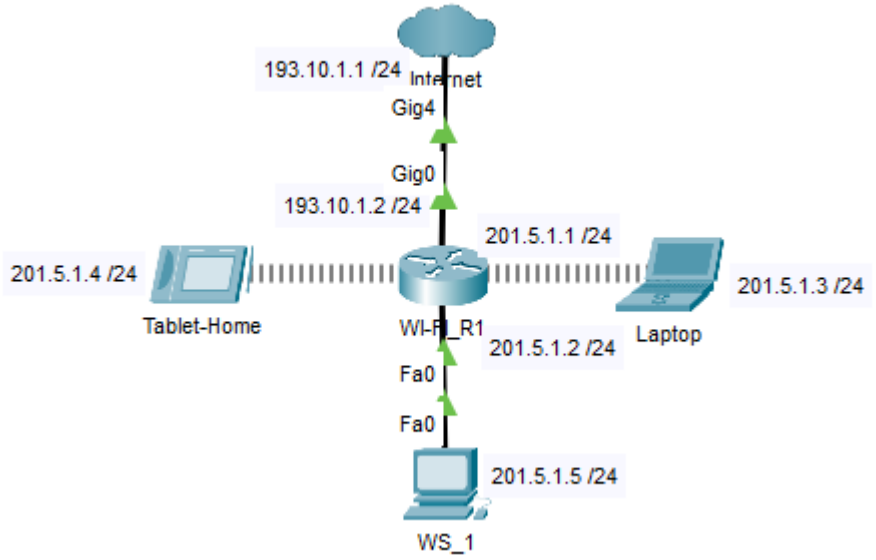

Рисунок 3.3 − Приклад топології мережі

Таблиця 2

Таблиця з’єднань

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор WI-FI_R1	Gig0	Internet	WAN
	Fa0	WS_1	Fa0
	Wireless0	Laptop	Wireless0
	Wireless0	Планшет	Wireless0
WS_1	Fa0	Маршрутизатор WI-FI_R1	Fa0
Laptop	Wireless0		Wireless0
Планшет	Wireless0		Wireless0

Таблиця 3

Таблиця адресації

Підмережа/ Пристрій	Інтерфейс/Мережевий адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа А	–	201.5.1.0	255.255.255.0	/24
Маршрутизатор WI-FI_R1	Wireless0	201.5.1.1	255.255.255.0	/24
	Fa0	201.5.1.2	255.255.255.0	/24
Laptop	Wireless0	201.5.1.3	255.255.255.0	/24
Планшет	Wireless0	201.5.1.4	255.255.255.0	/24
WS_1	Fa0	201.5.1.5	255.255.255.0	/24

Параметри для налагодження бездротової мережі для модельного прикладу наведені у табл. 4.

Таблиця 4

Параметри для налагодження бездротової мережі

Параметр	Значення
Назва мережі (SSID)	WI-FI_R1
Пароль	TestWIFI#1234
Метод аутентифікації	WPA
Налагодження	DHCP

Сценарій налагодження основних параметрів точки доступу на маршрутизаторі наведений нижче:

R1#service-module wlan-ap 0 session
ap>en
ap#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)#dot11 ssid WI-FI_R1
ap(config-ssid)#auth open
ap(config-ssid)#auth key-management wpa
ap(config-ssid)#wpa-psk ascii 0 TestWIFI#1234
ap(config-ssid)#guest-mode
ap(config-ssid)#exit
ap(config)#interface Dot11Radio0
ap(config-if)#no ip address
ap(config-if)#encryption mode ciphers aes-ccm
ap(config-if)#ssid WI-FI_R1
ap(config-if)#no shutdown
ap(config-if)#exit
ap(config)#exit
ap#exit

Для того, щоб повернутися з режиму точки доступу до консольного режиму маршрутизатора потрібно натиснути комбінацію Ctrl+Shift+6 та x.

Результати виконання команд моніторингу та діагностики роботи

З метою перегляду інформації про роботу бездротової мережі для розглянутого прикладу використано команди **show interface** (команди **show interface Dot11Radio 0** та **show show interface wlan-ap 0**), **show run** для даного прикладу покажуть аналогічні результати**).** Результати роботи цих команд для маршрутизатора WI-FI_R1 наведено відповідно на рис. 3.4–3.6.

```
ap#show run
Current configuration :
!
Version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ap
!
no ip ftp passive
bridge irb
```

```
!
dot11 ssid WI-FI_R1
authentication open
authentication key-management wpa
wpa-psk ascii 0 TestWIFI#1234
guest-mode
!
interface GigabitEthernet0
no ip address
bridge-group 1
!
interface Dot11Radio0
no ip address
bridge-group 1
encryption mode ciphers aes-ccm
ssid WI-FI_R1
!
interface Dot11Radio1
no ip address
bridge-group 1
shutdown
!
interface BVI1
mac-address 0001.64dc.ae01
ip address dhcp client-id GigabitEthernet 0
!
line con 0
!
line vty 0 4
login
!
end
```

Рисунок 3.4 – Результат виконання команди **show run** на маршрутизаторі WIFI_R1 в режимі точки доступу (ap)

```
ap#show interface Dot11Radio 0
Dot11Radio0 is up, line protocol is up (connected)
Hardware is 802.11N 2.4GHz Radio, address is 000A.F3A4.E602 (bia 000A.F3A4.E602)
MTU 1500 bytes, BW 54000 Kbit/sec, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/10066/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/30 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Рисунок 3.5 – Результат виконання команди **show interface Dot11Radio 0** на маршрутизаторі WIFI_R1 в режимі точки доступу (ap)

```
R1#show interface wlan-ap 0
wlan-ap0 is up, line protocol is up (connected)
Hardware is Lance, address is 00e0.b050.e208 (bia 00e0.b050.e208)
Description: Service module interface to manage the embedded AP
Internet address is 201.5.1.1/24
MTU 1500 bytes, BW 100000 Kbit, DLY 0 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Full-duplex, 100Mb/s, media type is RJ45
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Рисунок 3.6 – Результат виконання команди **show interface wlan-ap 0** на маршрутизаторі WIFI_R1

Модельний приклад налагодження функціонування бездротової комп'ютерної мережі на базі маршрутизатора Cisco 829

Розглянемо специфіку налагодження бездротових параметрів функціонування маршрутизатора Cisco моделі 829. Результат такого підключення наведений на рис. 3.7.

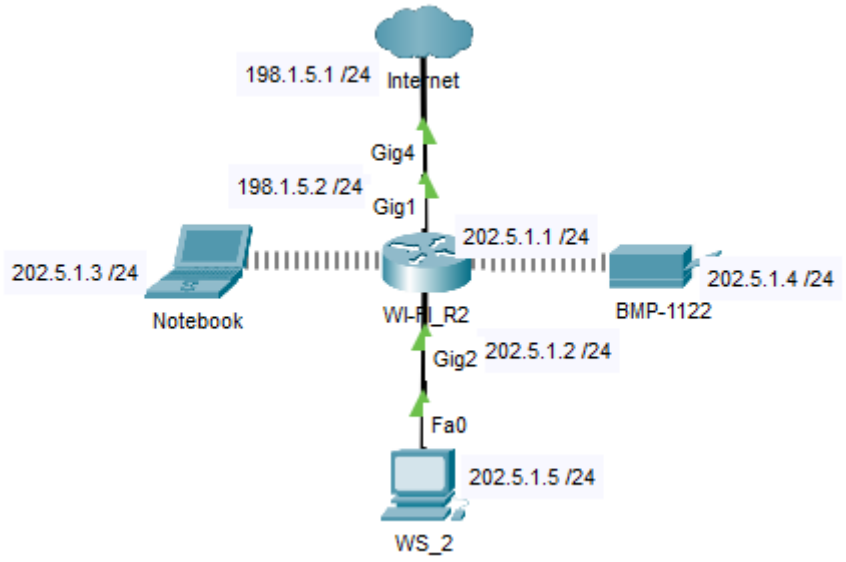

Рисунок 3.7 − Приклад топології мережі

Таблиця 5

Таблиця з'єднань

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор WI-FI_R2	Gig1	Internet	WAN
	Gig2	WS_2	Fa0
	Wireless0	Notebook	Wireless0
	Wireless0	BMP-1122	Wireless0
WS_3	Fa0	Маршрутизатор WI-FI_R2	Gig2
Notebook	Wireless0		Wireless0
BMP-1122	Wireless0		Wireless0

Таблиця 6

Таблиця адресації

Підмережа/ Пристрій	Інтерфейс/Мережевий адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа А	–	202.5.1.0	255.255.255.0	/24
Маршрутизатор WI-FI_R2	Wireless0	202.5.1.1	255.255.255.0	/24
	Gig2	202.5.1.2	255.255.255.0	/24
Notebook	Wireless0	202.5.1.3	255.255.255.0	/24
BMP-1122	Wireless0	202.5.1.4	255.255.255.0	/24
WS_2	Fa0	202.5.1.5	255.255.255.0	/24

Таблиця 7

Параметри для налагодження бездротової мережі

Параметр	Значення
Назва мережі (SSID)	WI-FI_R2
Пароль	TestWIFI#R2
Метод аутентифікації	WPA

Сценарій налагодження основних параметрів комутатора наведений нижче.

R2#conf t
R2(config)#interface wlan-ap0
R2(config-if)#ip address 202.5.1.1 255.255.255.0
R2(config-if)#end
R2#service-module wlan-ap 0 session
ap>en
ap#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)#dot11 ssid WI-FI_R2
ap(config-ssid)#auth open
ap(config-ssid)#auth key-management wpa
ap(config-ssid)#
ap(config-ssid)#wpa-psk ascii 0 TestWIFI#R2
ap(config-ssid)#guest-mode
ap(config-ssid)#exit
ap(config)#interface Dot11Radio0

ap(config-if)#no ip address
ap(config-if)#encryption mode ciphers aes-ccm
ap(config-if)#ssid WI-FI_R2
ap(config-if)#no shutdown

Для того, щоб повернутися з режиму точки доступу до консольного режиму маршрутизатора потрібно натиснути комбінацію Ctrl+Shift+6 та x.

Результати виконання команд моніторингу та діагностики роботи

З метою перегляду інформації про роботу бездротової мережі для розглянутого прикладу використано команди **show interface** (команди **show interface Dot11Radio 0** та **show show interface wlan-ap 0**), **show run** для даного прикладу покажуть аналогічні результати**).** Результати роботи цих команд для маршрутизатора WI-FI_R2 наведено відповідно на рис. 3.8–3.10.

```
ap#show run
Current configuration :
!
version 15.3
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname ap
!
!
!
no ip ftp passive
bridge irb
!
dot11 ssid WI-FI_R2
authentication open
authentication key-management wpa
wpa-psk ascii 0 TestWIFI#R2
guest-mode
!
interface GigabitEthernet0
description the embedded AP GigabitEthernet 0 is an internal interface
connecting AP with the host router
no ip address
bridge-group 1
!
interface Dot11Radio0
no ip address
bridge-group 1
encryption mode ciphers aes-ccm
ssid WI-FI_R2
!
interface Dot11Radio1
no ip address
bridge-group 1
shutdown
!
interface BVI1
mac-address 0080.0bc2.0201
no ip address
ip address dhcp client-id GigabitEthernet 0
!
line con 0
!
line vty 0 4
login
!
end
```

Рисунок 3.8 − Результат виконання команди **show run**
на маршрутизаторі WI-FI_R2 в режимі точки доступу (ap)

```
ap#show interface Dot11Radio 0
Dot11Radio0 is up, line protocol is up (connected)
Hardware is 802.11N 2.4GHz Radio, address is 0090.0CC8.0702 (bia 0090.0CC8.0702)
MTU 1500 bytes, BW 54000 Kbit/sec, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/10066/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/30 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Рисунок 3.9 – Результат виконання команди **show interface Dot11Radio 0** на маршрутизаторі WI-FI_R2 в режимі точки доступу (ap)

```
R2#show interface wlan-ap 0
wlan-ap0 is up, line protocol is up (connected)
Hardware is Lance, address is 0030.f28b.b606 (bia 0030.f28b.b606)
Internet address is 202.5.1.1/24
MTU 1500 bytes, BW 100000 Kbit, DLY 0 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Full-duplex, 100Mb/s, media type is RJ45
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Рисунок 3.10 – Результат виконання команди **show interface wlan-ap 0** на маршрутизаторі WI-FI_R2

Налагодження DHCP на маршрутизаторах Cisco моделі 829 має свої особливості. Це пов’язано з необхідністю налаштовувати BVI (Bridge group Virtual Interface).

```
R2#conf t
R2(config)#ip dhcp pool R2
R2(dhcp-config)#network 202.5.1.0 255.255.255.0
R2(dhcp-config)#dns-server 8.8.8.8
R2(dhcp-config)#default-router 202.5.1.1
R2(dhcp-config)#exit
R2(config)#ip dhcp excluded-address 202.5.1.1

R2(config)#int wlan-ap0
R2(config-if)#ip unnumbered vlan1
R2(config-if)#exit
R2(config)#interface vlan1
R2(config-if)#ip address 202.5.1.10 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#ip dhcp excluded-address 202.5.1.10
R2(config-if)#exit

ap>enable
ap#conf t
ap(config)#int bvi1
ap(config-if)# ip address 202.5.1.1 255.255.255.0
ap(config-if)#no shutdown
```

Модельний приклад налагодження функціонування бездротової комп'ютерної мережі на базі комутатора Cisco 2811 із модулем HWIC-AP-AG-B

Розглянемо специфіку налагодження бездротових параметрів функціонування маршрутизатора Cisco моделі 2811 із модулем HWIC-AP-AG-B. Результат такого підключення наведений на рис. 3.11.

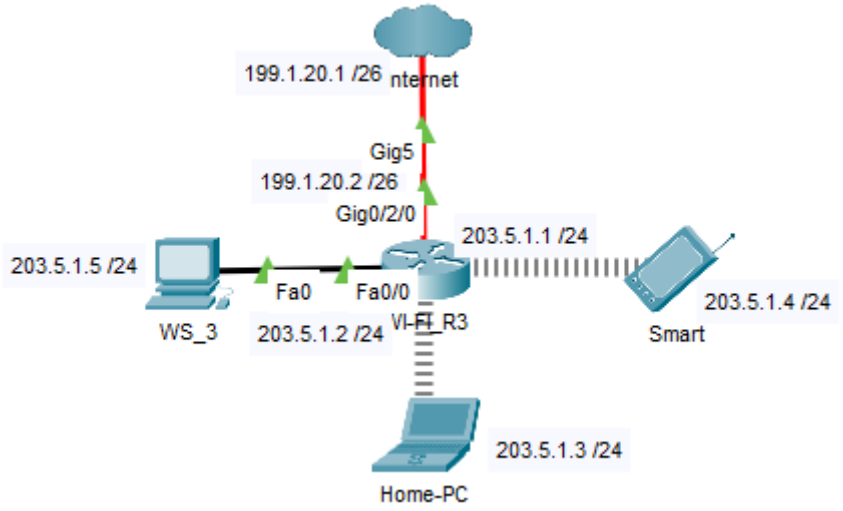

Рисунок 3.11 – Приклад топології мережі

Таблиця 8

Таблиця з'єднань

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор WI-FI_R3	Gig0/2/0	Internet	WAN
	Fa0/0	WS_3	Fa0
	Wireless0	Home-PC	Wireless0
	Wireless0	Smart	Wireless0
WS_3	Fa0	Маршрутизатор WI-FI_R3	Fa0/0
Home-PC	Wireless0		Wireless0
Smart	Wireless0		Wireless0

Таблиця 9

Таблиця адресації

Підмережа/ Пристрій	Інтерфейс/Мережевий адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа А	–	203.5.1.0	255.255.255.0	/24
Маршрутизатор WI-FI_R3	Wireless0	203.5.1.1	255.255.255.0	/24
	Fa0/1	203.5.1.2	255.255.255.0	/24
Home-PC	Wireless0	203.5.1.3	255.255.255.0	/24
Smart	Wireless0	203.5.1.4	255.255.255.0	/24
WS_2	Fa0	203.5.1.5	255.255.255.0	/24

Таблиця 10

Параметри для налагодження бездротової мережі

Параметр	Значення
Назва мережі (SSID)	WI-FI_R3
Пароль	TestWIFI#R3
Метод аутентифікації	WPA

Сценарій налагодження основних параметрів комутатора наведений нижче.

R3#
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#dot11 ssid WI-FI_R3
R3(config-ssid)#auth open
R3(config-ssid)#auth key-management wpa
R3(config-ssid)#wpa-psk ascii 0 TestWIFI#R3
R3(config-ssid)#guest-mode
R3(config-if)#exit
R3(config)#interface Dot11Radio0/0/0
R3(config-if)#no ip address
R3(config-if)#encryption mode ciphers aes-ccm
R3(config-if)#ssid WI-FI_R3
R3(config-if)#no shut
R3(config-if)#end
R3#copy running-config startup-config

Результати виконання команд моніторингу та діагностики роботи

З метою перегляду інформації про роботу бездротової мережі для розглянутого прикладу використано команди **show interface** (команди **show interface Dot11Radio 0/0/0**), **show dot11** для даного прикладу покажуть аналогічні результати**)**. Результати роботи цих команд для маршрутизатора WI-FI_R3 наведено відповідно на рис. 3.12–3.13.

```
R3#show interface Dot11Radio0/0/0
Dot11Radio0/0/0 is up, line protocol is up (connected)
Hardware is 802.11G Radio, address is 00d0.d366.3e01 (bia 00d0.d366.3e01)
MTU 1500 bytes, BW 11000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 11Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/30 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
```

Рис. 3.12 – Результат виконання команди **show interface Dot11Radio0/0/0** на маршрутизаторі WIFI_R3

```
R3#show dot11 interface

Interface Dot11Radio0/0/0 Statistics (Cumulative Total/Last 5 Seconds):
RECEIVER TRANSMITTER
Host Rx Bytes: 0 / 0 Host Tx Bytes: 0 / 0
Unicasts Rx: 0 / 0 Unicasts Tx: 0 / 0
Unicasts to host: 0 / 0 Unicasts by host: 0 / 0
Broadcasts Rx: 0 / 0 Broadcasts Tx: 0 / 0
Beacons Rx: 0 / 0 Beacons Tx: 0 / 0
Prob Req Rx: 0 / 0 Prob Resp Tx: 0 / 0
Broadcasts to host: 0 / 0 Broadcasts by host: 0 / 0
Multicasts Rx: 0 / 0 Multicasts Tx: 0 / 0
Multicasts to host: 0 / 0 Multicasts by host: 0 / 0
Mgmt Packets Rx: 0 / 0 Mgmt Packets Tx: 0 / 0
RTS received: 0 / 0 RTS transmitted: 0 / 0
Duplicate frames: 0 / 0 CTS not received: 0 / 0
CRC errors: 0 / 0 Unicast Fragments Tx: 0 / 0
WEP errors: 0 / 0 Retries: 0 / 0
Buffer full: 0 / 0 Packets one retry: 0 / 0
Host buffer full: 0 / 0 Packets > 1 retry: 0 / 0
Header CRC errors: 0 / 0 Protocol defers: 0 / 0
Invalid header: 0 / 0 Energy detect defers: 0 / 0
Length invalid: 0 / 0 Jammer detected: 0 / 0
Incomplete fragments: 0 / 0 Packets aged: 0 / 0
Rx Concats: 0 / 0 Tx Concats: 0 / 0
Interface Dot11Radio0/0/1 Statistics (Cumulative Total/Last 5 Seconds):
RECEIVER TRANSMITTER
Host Rx Bytes: 0 / 0 Host Tx Bytes: 0 / 0
Unicasts Rx: 0 / 0 Unicasts Tx: 0 / 0
Unicasts to host: 0 / 0 Unicasts by host: 0 / 0
Broadcasts Rx: 0 / 0 Broadcasts Tx: 0 / 0
Beacons Rx: 0 / 0 Beacons Tx: 0 / 0
Prob Req Rx: 0 / 0 Prob Resp Tx: 0 / 0
Broadcasts to host: 0 / 0 Broadcasts by host: 0 / 0
```

```
Multicasts Rx: 0 / 0 Multicasts Tx: 0 / 0
Multicasts to host: 0 / 0 Multicasts by host: 0 / 0
Mgmt Packets Rx: 0 / 0 Mgmt Packets Tx: 0 / 0
RTS received: 0 / 0 RTS transmitted: 0 / 0
Duplicate frames: 0 / 0 CTS not received: 0 / 0
CRC errors: 0 / 0 Unicast Fragments Tx: 0 / 0
WEP errors: 0 / 0 Retries: 0 / 0
Buffer full: 0 / 0 Packets one retry: 0 / 0
Host buffer full: 0 / 0 Packets > 1 retry: 0 / 0
Header CRC errors: 0 / 0 Protocol defers: 0 / 0
Invalid header: 0 / 0 Energy detect defers: 0 / 0
Length invalid: 0 / 0 Jammer detected: 0 / 0
Incomplete fragments: 0 / 0 Packets aged: 0 / 0
Rx Concats: 0 / 0 Tx Concats: 0 / 0

LOST PARENT COUNTS ASSOCIATION STATISTICS
Maximum retries: 0 / 0 SSID mismatched: 0 / 0
No beacons: 0 / 0 Not specified AP: 0 / 0
Average retry level: 0 / 0 Rates mismatched: 0 / 0
Deauthenicated: 0 / 0 Privacy mismatched: 0 / 0
Disassociated: 0 / 0 Authentication rejects: 0 / 0
Time base lost: 0 / 0 Association timeout: 0 / 0
Host request: 0 / 0 LEAP successes: 0 / 0
Better parent found: 0 / 0 LEAP failures: 0 / 0
LEAP timeouts: 0 / 0
LEAP key len fails: 0 / 0
PHY element mismatch: 0 / 0
WPA IE mismatch: 0 / 0
```

Рисунок 3.13 – Результат виконання команди **show dot11 interface** на маршрутизаторі WIFI_R3

Модельний приклад налагодження функціонування відкритої бездротової комп'ютерної мережі на базі комутатора Cisco 2811 із модулем HWIC-AP-AG-B

Розглянемо специфіку налагодження бездротових параметрів функціонування маршрутизатора Cisco моделі 2811 із модулем HWIC-AP-AG-B. Результат такого підключення наведений на рис. 3.14.

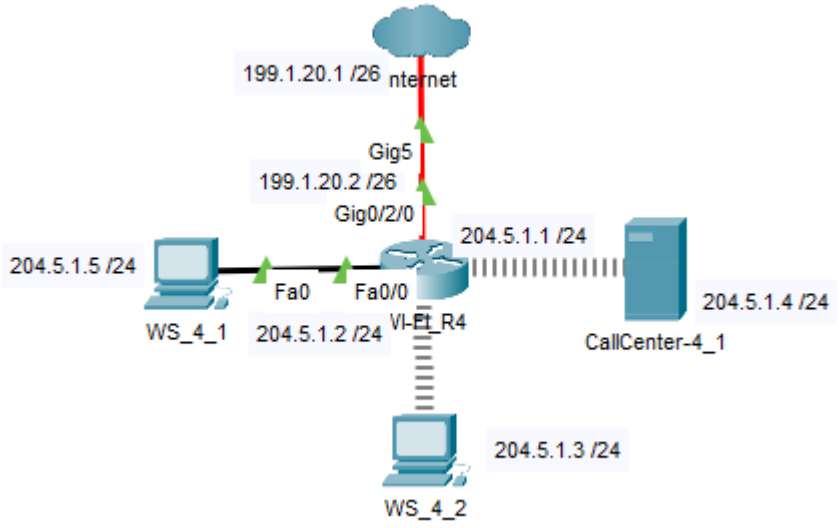

Рисунок 3.14 – Приклад топології мережі

Важливо! Кінцеві пристрої, підключення яких до Wi-Fi відбувається через меню Config – не підтримують зв'язок із точками доступу без парольного захисту.

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R4
R4(config)#dot11 ssid WI-FI_R4
R4(config-ssid)#auth open
R4(config-ssid)#guest-mode
R4(config-ssid)#exit
R4(config)#interface Dot11Radio0/0/0
R4(config-if)#ssid WI-FI_R4
R4(config-if)#no shut
R4(config-if)#
R4(config-if)#end
R4#copy running-config startup-config
R4#
```

Таблиця 11

Таблиця з'єднань

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор WI-FI_R4	Gig0/2/0	Internet	WAN
	Fa0/0	WS_4_1	Fa0
	Wireless0	WS_4_2	Wireless0
	Wireless0	CallCenter-4_1	Wireless0
WS_4_1	Fa0	Маршрутизатор WI-FI_R4	Fa0/0
WS_4_2	Wireless0		Wireless0
CallCenter-4_1	Wireless0		Wireless0

Таблиця 12

Таблиця адресації

Підмережа/ Пристрій	Інтерфейс/Мережевий адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа A	–	204.5.1.0	255.255.255.0	/24
Маршрутизатор WI-FI_R4	Wireless0	204.5.1.1	255.255.255.0	/24
	Fa0/1	204.5.1.2	255.255.255.0	/24
Notebook	Wireless0	204.5.1.3	255.255.255.0	/24
CallCenter-4_1	Wireless0	204.5.1.4	255.255.255.0	/24
WS_2	Fa0	204.5.1.5	255.255.255.0	/24

Таблиця 13

Параметри для налагодження бездротової мережі

Параметр	Значення
Назва мережі (SSID)	WI-FI_R4
Пароль	–
Метод аутентифікації	–

Модельний приклад налагодження функціонування бездротового модулю на базі Laptop

1. На вкладці «Physical» вимикаємо ноутбук. (Рис. 3.15)
2. Перетягуємо модуль із ноутбука в ліву область. (Рис 3.15)
3. Перетягуємо модуль «WPC300N» в пусте місце на ноутбуці. (Рис 3.16)
4. Вмикаємо ноутбук. (Рис. 3.16)

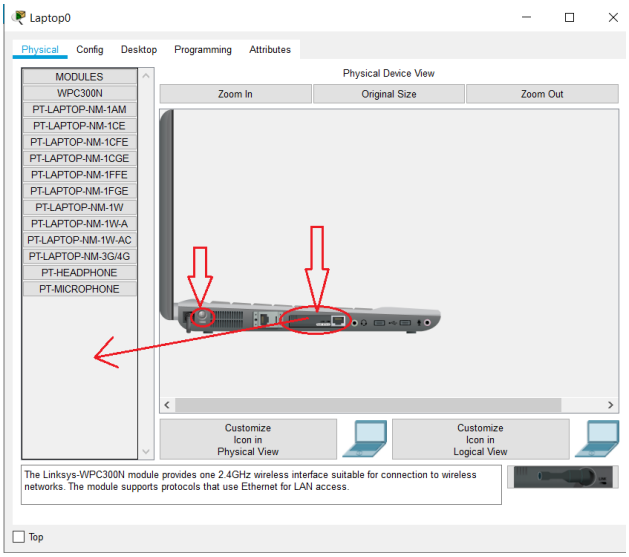

Рисунок 3.15

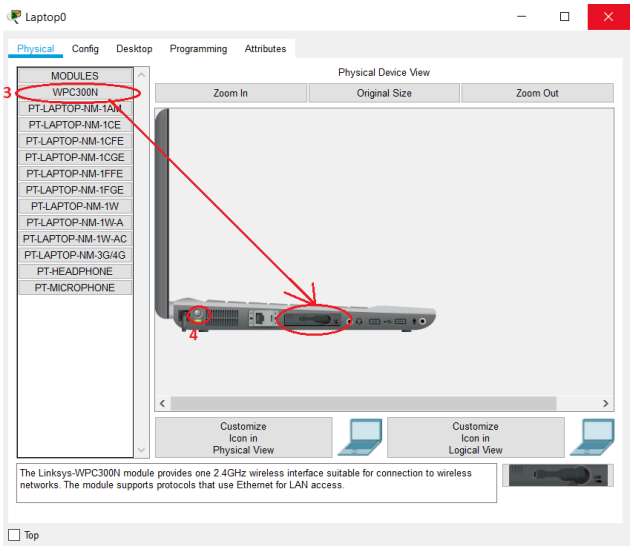

Рисунок 3.16

5. На вкладці Desktop натискаємо «PC Wireless». (Рис. 3.17)
6. У відкритому вікні обираємо вкладку «Connect» та обираємо нашу мережі і натискаємо на кнопку «Connect» (Рис. 3.18)
7. Обираємо стандарт захисту мережі та вводимо пароль мережі. Натискаємо «Connect». (Рис. 3.19)

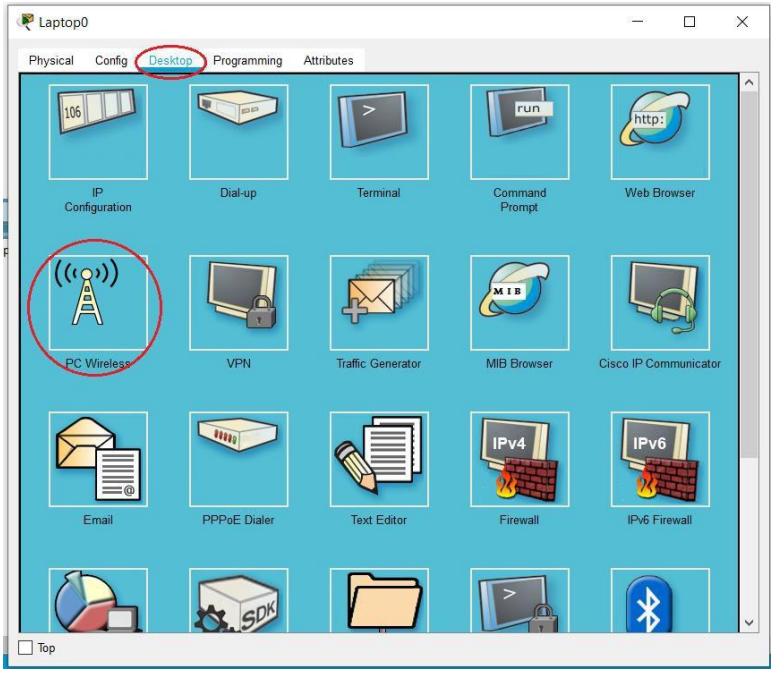

Рисунок 3.17 – Перехід до меню пошуку бездротових мереж

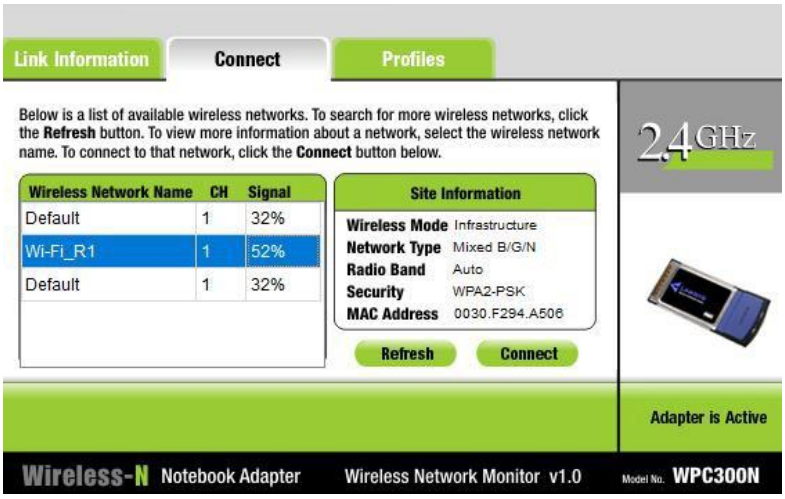

Рисунок 3.18 – Пошук Wi-Fi мережі

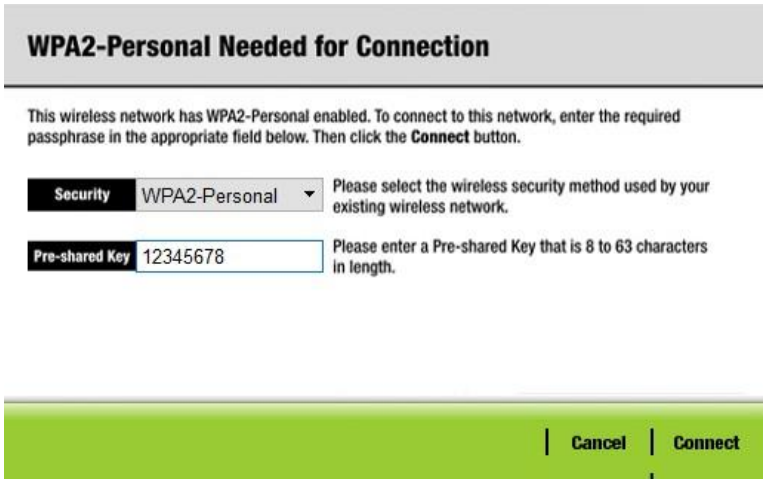

Рисунок 3.19 – Підключення до мережі

Завдання на лабораторну роботу:

1. У середовищі програмного симулятора/емулятора створити проєкт мережі (рис. 3.20). Під час побудови мережі звернути увагу на вибір моделей мережевих пристроїв, мережевих модулів та адаптерів, а також мережевих з'єднань (на рисунку мережеві з'єднання показані у загальному вигляді). Для вибору скористатися даними табл. 14 та табл. 15. Для побудованої мережі заповнити описову таблицю, яка аналогічна табл. 2.

2. Ім'я мережі (SSID) складається з R_G_N_X та пароля MyWiFi_R_G_N_X

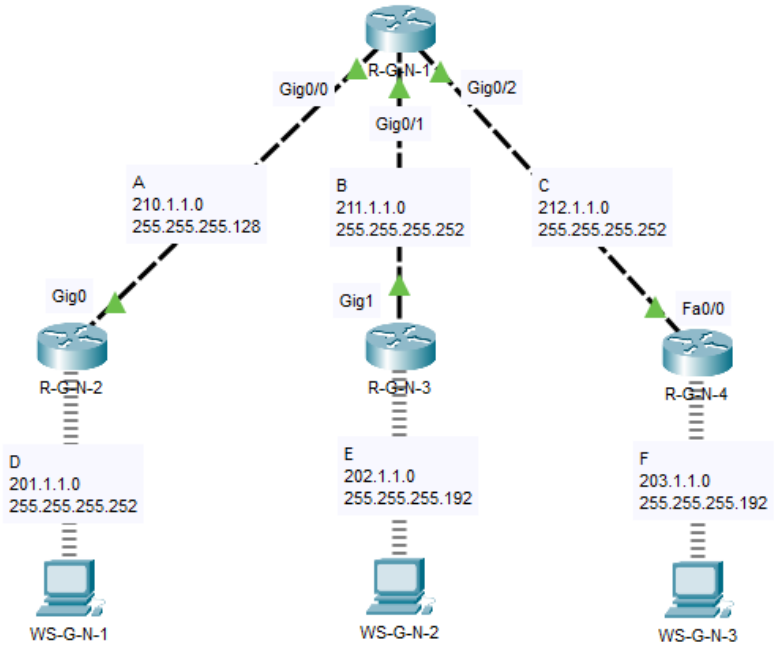

Рисунок 3.20. Проєкт мережі

Таблиця 14

Дані для адресації підмереж (каналів)

№ варіанта	Підмережа A		Підмережа B		Підмережа C		Підмережа D		Підмережа E		Підмережа F	
	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс
1	193.G.N.0	/27	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/24	198.G.N.0	/24
2	193.G.N.64	/27	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/25	198.G.N.0	/25
3	193.G.N.128	/27	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/26	198.G.N.0	/26
4	193.G.N.192	/27	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/27	198.G.N.0	/27
5	193.G.N.0	/28	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/28	198.G.N.0	/28
6	193.G.N.32	/28	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/24	198.G.N.0	/24
7	193.G.N.64	/28	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/25	198.G.N.0	/25
8	193.G.N.96	/28	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/26	198.G.N.0	/26
9	193.G.N.128	/28	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/27	198.G.N.0	/27
10	193.G.N.160	/28	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/28	198.G.N.0	/28
11	193.G.N.192	/28	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/24	198.G.N.0	/24
12	193.G.N.224	/28	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/25	198.G.N.0	/25
13	193.G.N.0	/25	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/26	198.G.N.0	/26
14	193.G.N.0	/26	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/27	198.G.N.0	/27
15	193.G.N.128	/26	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/28	198.G.N.0	/28
16	193.G.N.0	/27	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/24	198.G.N.0	/24
17	193.G.N.64	/27	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/25	198.G.N.0	/25
18	193.G.N.128	/27	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/26	198.G.N.0	/26
19	193.G.N.192	/27	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/27	198.G.N.0	/27
20	193.G.N.0	/26	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/28	198.G.N.0	/28
21	193.G.N.32	/28	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/24	198.G.N.0	/24
22	193.G.N.64	/28	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/25	198.G.N.0	/25
23	193.G.N.96	/28	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/26	198.G.N.0	/26
24	193.G.N.128	/28	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/27	198.G.N.0	/27
25	193.G.N.160	/28	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/29	197.G.N.0	/28	198.G.N.0	/28

Таблиця 15

Параметри налагодження

№ варіанту	Маршрутизатор R_G_N_2	Маршрутизатор R_G_N_3	Маршрутизатор R_G_N_4	Аутентифікація R_G_N_2	Аутентифікація R_G_N_3	Аутентифікація R_G_N_4
1	819	829	2811	WEP	WPA2-PSK	Open
2	829	2811	819	WPA2-PSK	Open	WPA2-PSK
3	2811	819	829	Open	WPA2-PSK	Open
4	819	829	2811	WPA2-PSK	Open	WEP
5	829	2811	819	Open	WEP	Open
6	2811	819	829	WEP	Open	WEP
7	819	829	2811	Open	WEP	WPA2-PSK
8	829	2811	819	WEP	WPA2-PSK	WEP
9	2811	819	829	WPA2-PSK	WEP	WPA2-PSK
10	819	829	2811	WEP	WPA2-PSK	Open
11	829	2811	819	WPA2-PSK	Open	WPA2-PSK
12	2811	819	829	Open	WPA2-PSK	Open
13	819	829	2811	WPA2-PSK	Open	WEP
14	829	2811	819	Open	WEP	Open
15	2811	819	829	WEP	Open	WEP
16	819	829	2811	Open	WEP	WPA2-PSK
17	829	2811	819	WEP	WPA2-PSK	WEP
18	2811	819	829	WPA2-PSK	WEP	WPA2-PSK
19	819	829	2811	WEP	WPA2-PSK	Open
20	829	2811	819	WPA2-PSK	Open	WPA2-PSK
21	2811	819	829	Open	WPA2-PSK	Open
22	819	829	2811	WPA2-PSK	Open	WEP
23	829	2811	819	Open	WEP	Open
24	2811	819	829	WEP	Open	WEP
25	819	829	2811	Open	WEP	WPA2-PSK

Таблиця 16

Механізм адресації кінцевих вузлів локальних мереж

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

Контрольні питання:

1. Які завдання вирішують бездротові мережі?
2. Які є стандарти захисту мереж Wi-Fi?
3. У чому відмінність між стандартами WEP та WPA?
4. У чому відмінність між стандартами WPA та WPA2?
5. Який стандарт найбільш оптимальний для використання в дома?
6. Який стандарт найбільш оптимальний для використання в великій компанії?
7. Яку команду необхідно виконати для налагодження захищеного доступу до Wi-Fi за допомогою WPA-PSK?
8. Який бездротовий модуль використовувався для налагодження бездротової мережі у маршрутизаторі Cisco 2811?
9. За допомогою якої команди потрібно входити в сервісний режим на Cisco 819 та 829?
10. Як налагодити відкриту бездротову мережу?

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. 4.1, 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 4.1 – 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. 4.2 – 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.

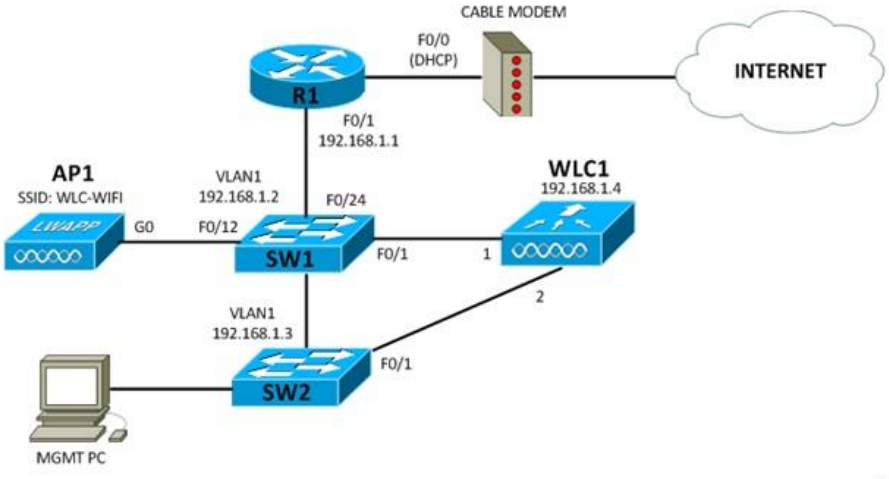

Рисунок 4.2 – Типова контролерна топологія та мережеві підключення

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. 4.3). 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.

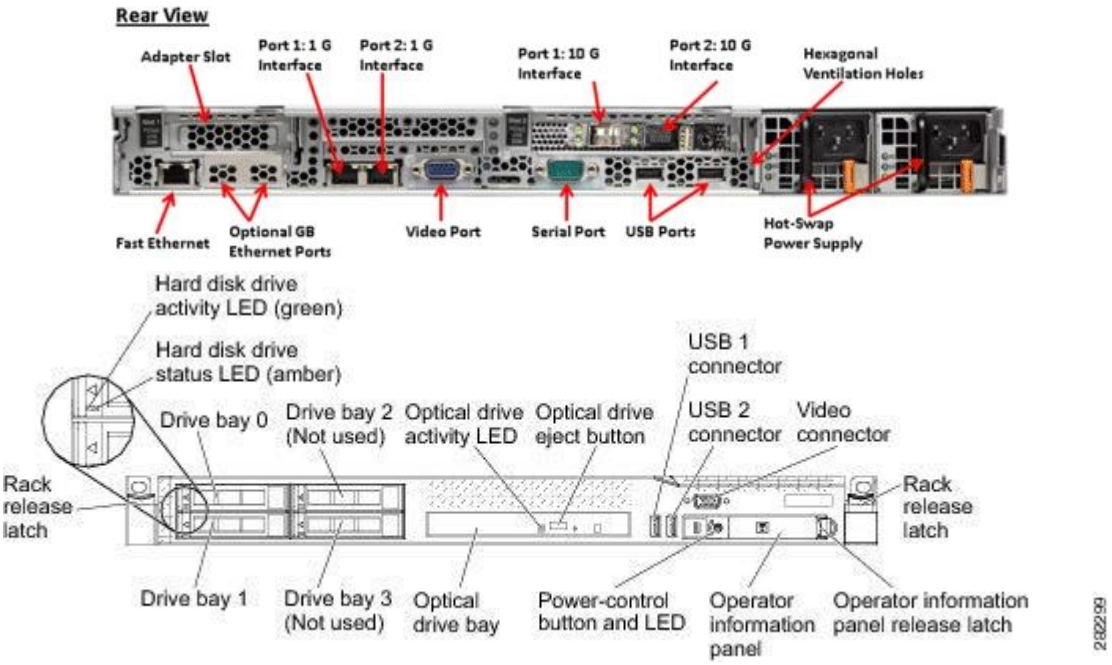

Рисунок 4.3 – Бездротовий контролер Cisco Flex 7500

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. 4.4). 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.

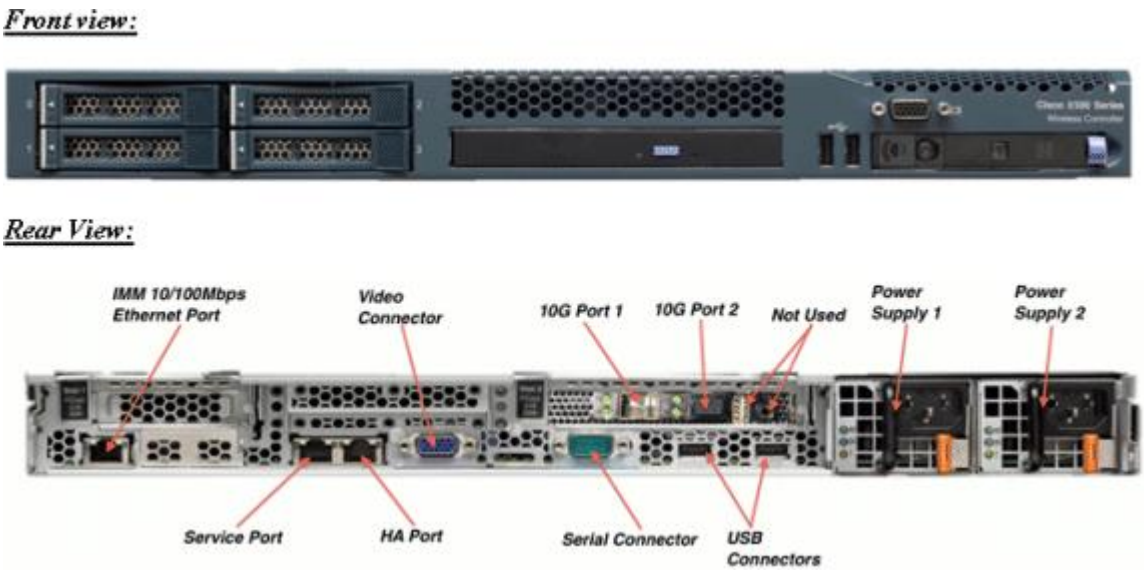

Рисунок 4.4 – Бездротовий контролер Cisco серії 8500 – 8510

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, двосторонній курс ліміту руху транспорту;
- 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 перенаправляти консоль із швидкістю 9600, що імітує термінал VT100 без керування потоком. Контролер 8500 має таку ж завантажувальну послідовність, що й існуючі контролери (рис. 4.5).

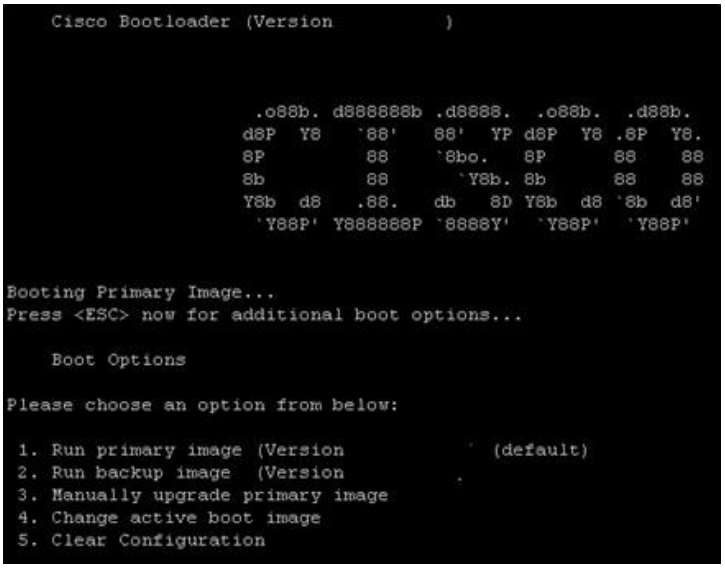

Рисунок 4.5 – Запуск бездротового контролера 8510

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. 4.6:

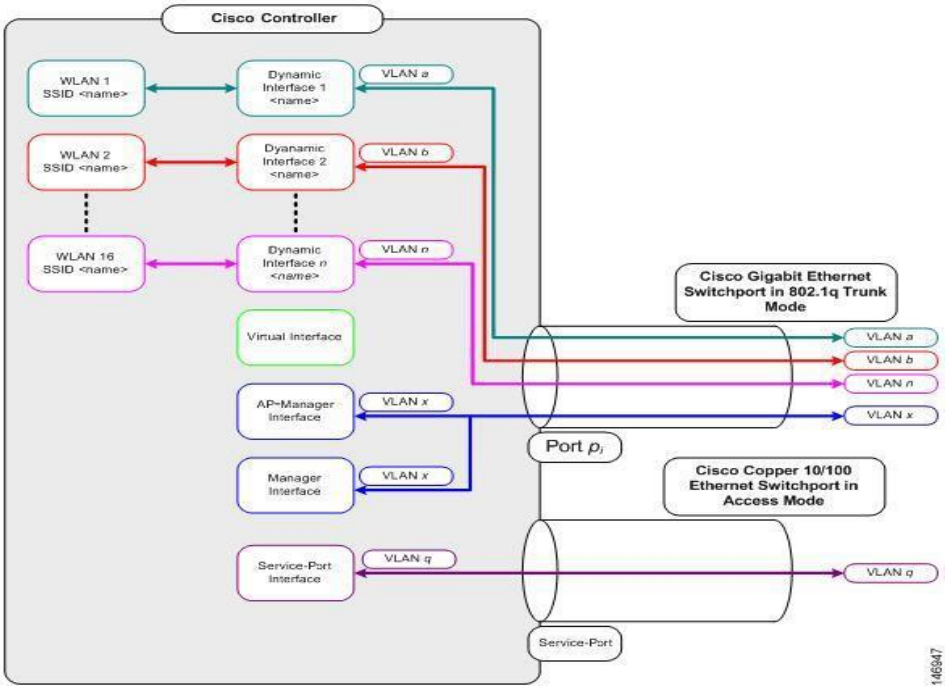

Рисунок 4.6 – Схематичний приклад VLAN, WLC

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. 4.7.

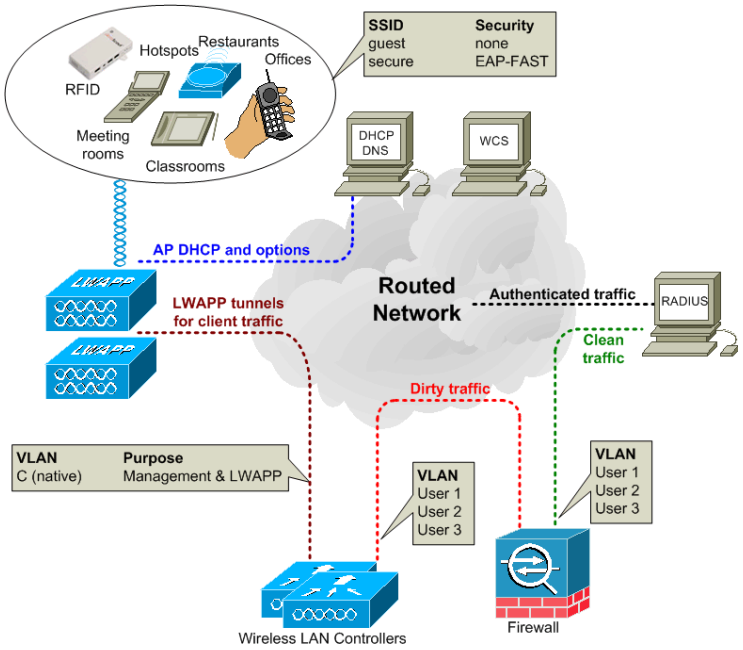

Рисунок 4.7 – Схематична побудова LightWeight Access Point

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. 4.8).

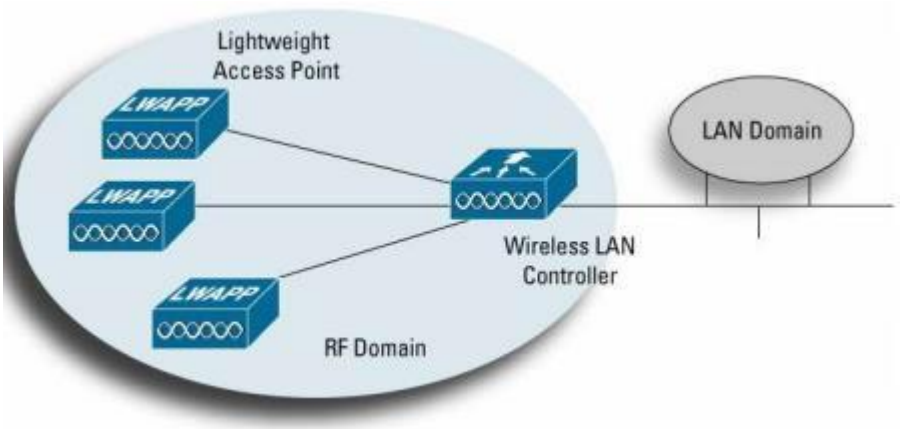

Рисунок 4.8 – WLAN системи централізованого інтелекту для широкого корпоративного управління підприємством та управління політикою

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.

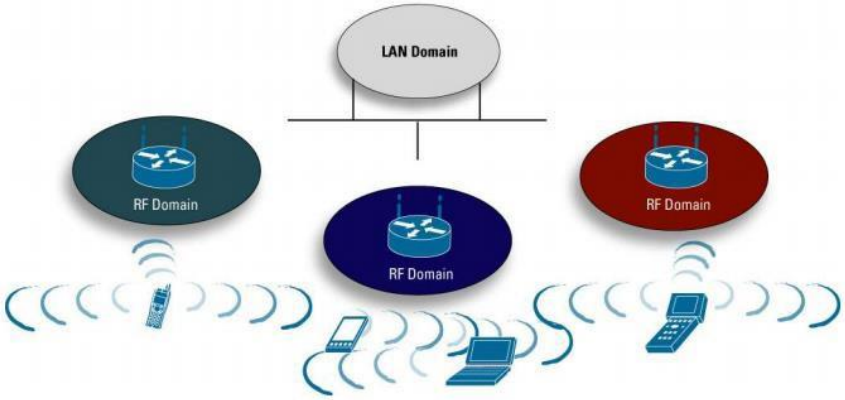

Рисунок 4.9 – Архітектура однорідної мережі WLAN обмежує продуктивність, керованість та безпеку

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 тегуванння 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 інформаціїпро VLAN 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

Продовження 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. 4.10.

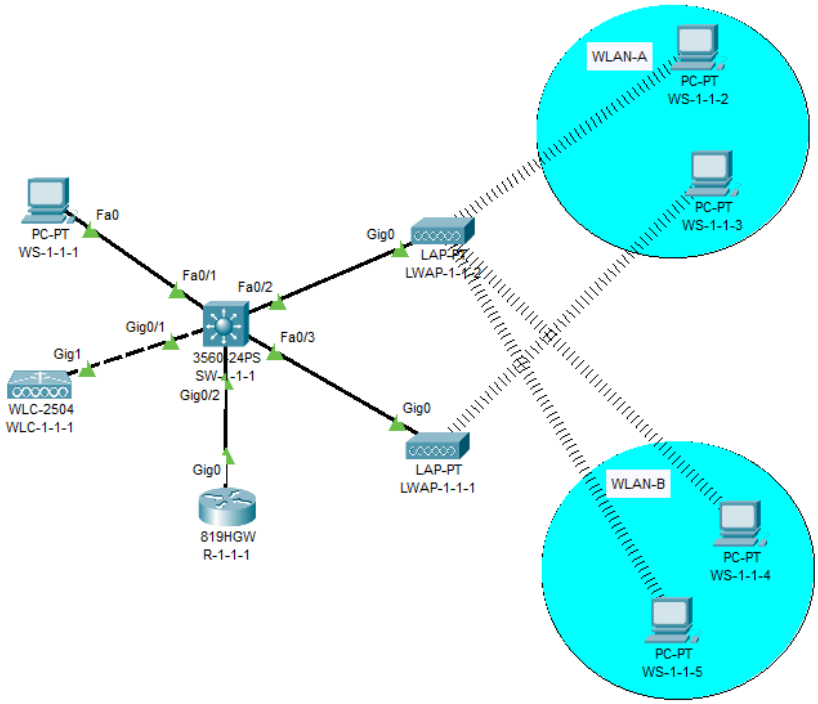

Рисунок 4.10 – Приклад налагодження Cisco WLC 2504

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	192.168.1.200	192.168.1.200	192.168.1.1
Mask	255.255.255.0	255.255.255.0	255.255.255.0
Default gateway	192.168.1.1	192.168.1.200	—
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 100
Switch(config-if)# ip address 192.168.1.2 255.255.255.0
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 192.168.1.2
Switch(config)# ip dhcp excluded-address 192.168.1.100

Switch(config)# ip dhcp excluded-address 192.168.1.200
Switch(config)# service dhcp

Підключіться до WLC 2504, використовуючи веб-браузер ноутбука керування, задаючи адресу: 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 використовується протокол HTTP (незахищений), а не HTTPS (рис. 4.11).

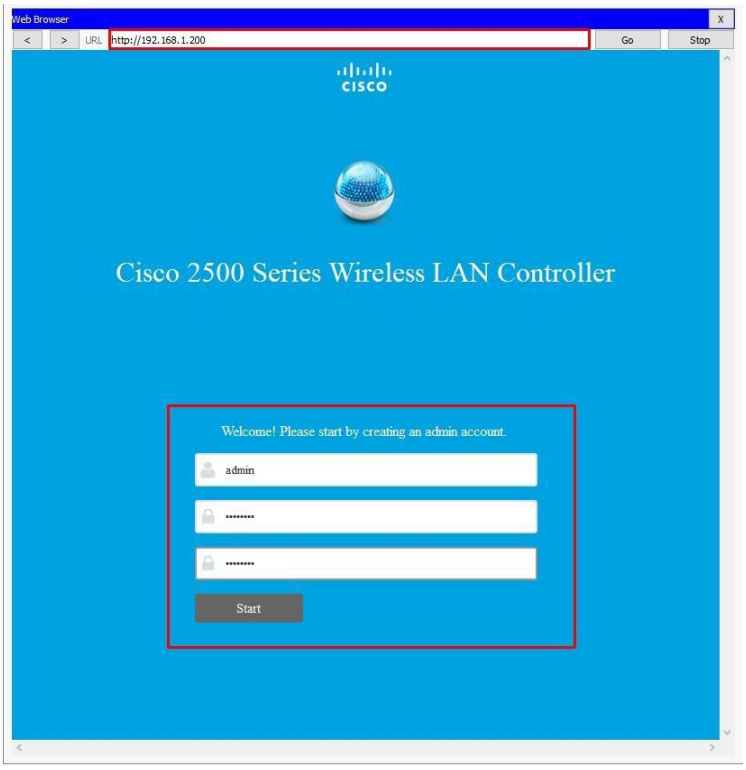

Рисунок 4.11 – Початкові налаштування Wireless Lan Controller

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, наприклад 192.168.1.1) (рис. 4.12). Після цього натисніть «Next», де Ви можете подивитись задані налаштування перед збереженням, як показано на рис. 4.13. 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. 4.14. Натискайте «OK», після чого можете закривати бразузер. Необхідно прискорити час симуляції мережі, так як процес перезавантаження WLC займає досить багато часу.

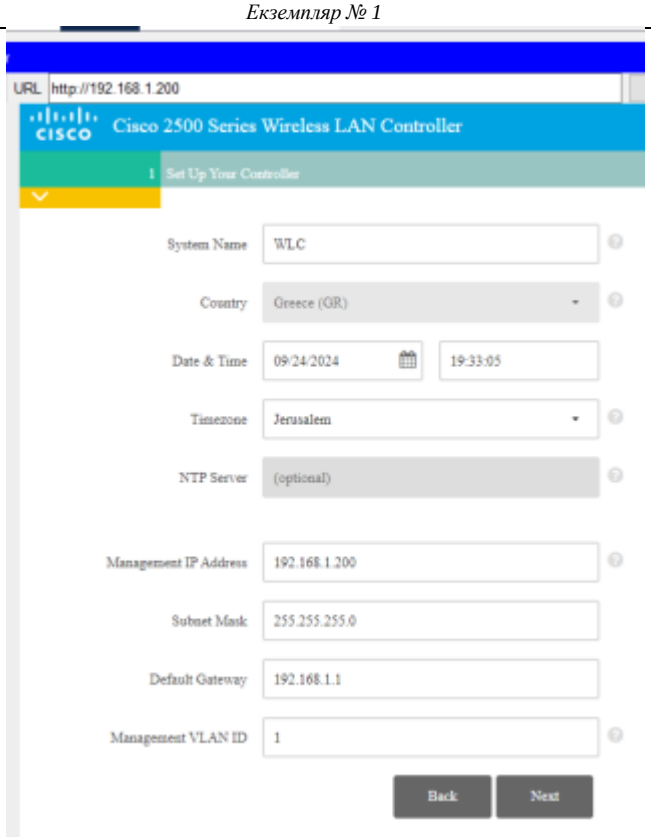

Рисунок 4.12 – Налаштування WLC

Рисунок 4.13 – Завершальний процес застосування

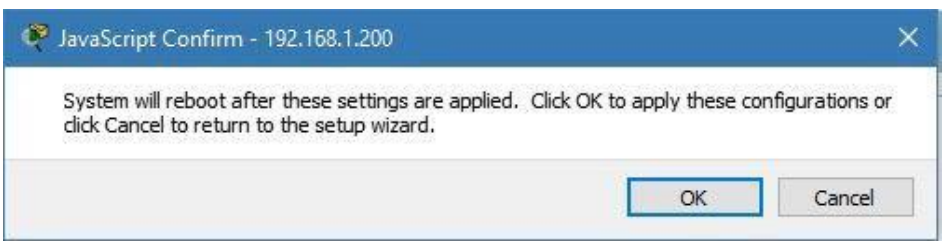

Рисунок 4.14 – Підтвердження перезавантаження WLC

Після завершення початкового процесу налаштування, підключіться повторно до Cisco WLC за допомогою **HTTPS** (https://192.168.1.200) (рис. 4.15) . 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 4.15 – 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. 4.16).

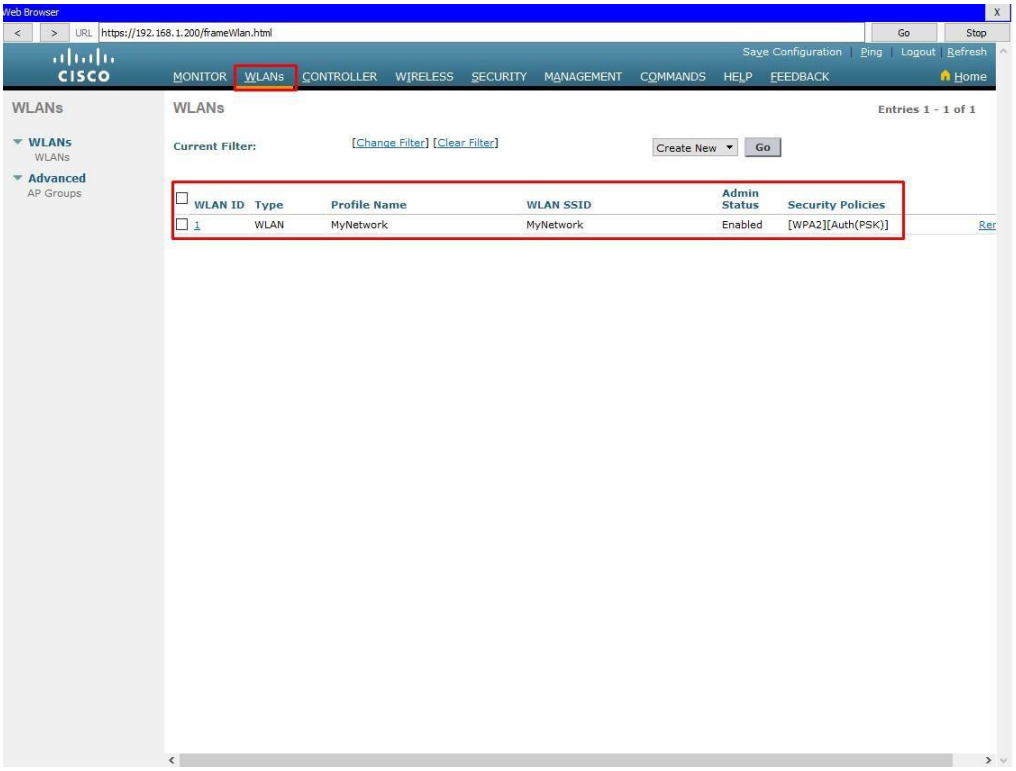

Рисунок 4.16 – Створення WLAN

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. 4.17.

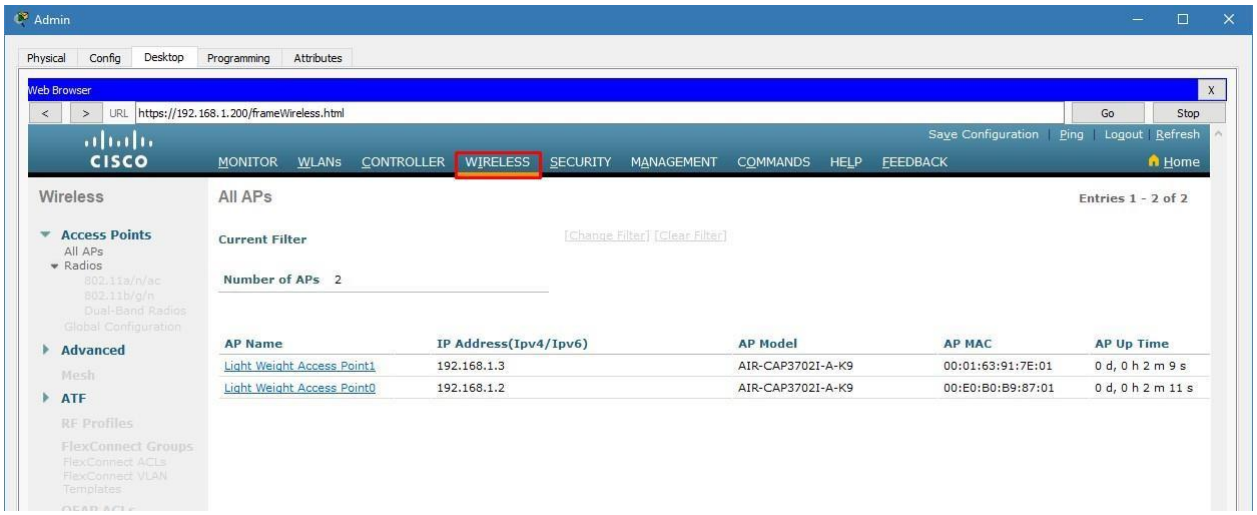

Рисунок 4.17 – Успішно зареєстровані точки доступу

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. 4.18.

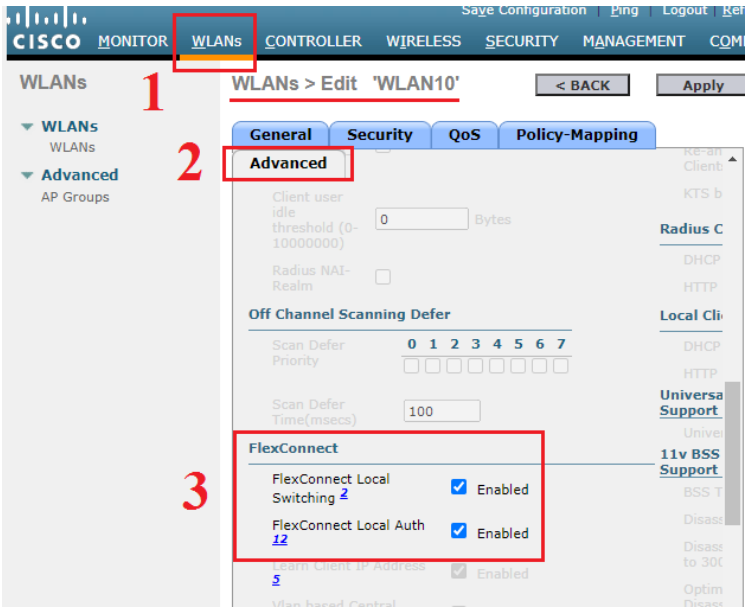

Рисунок 4.18 – Налаштування FlexConnect для WLAN

Для розподіленого підключення робочих станцій до точок доступу, варто зменшити радіус їхньої дії до 50 м, як показано на рис. 4.19.

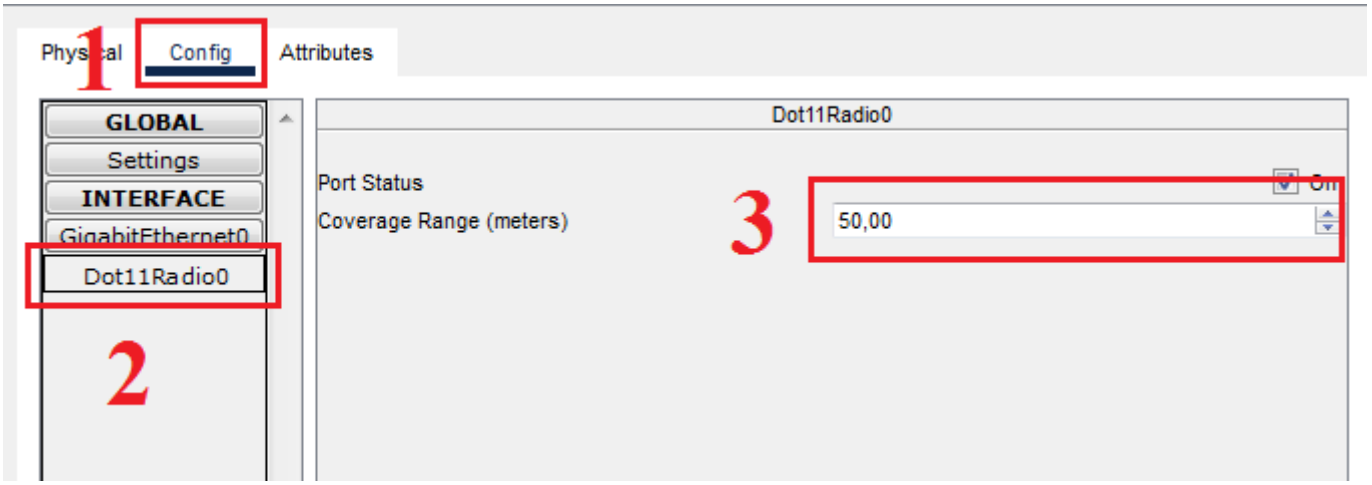

Рисунок 4.19 – Налаштування радіусу дії точки доступу

Завдання на лабораторну роботу

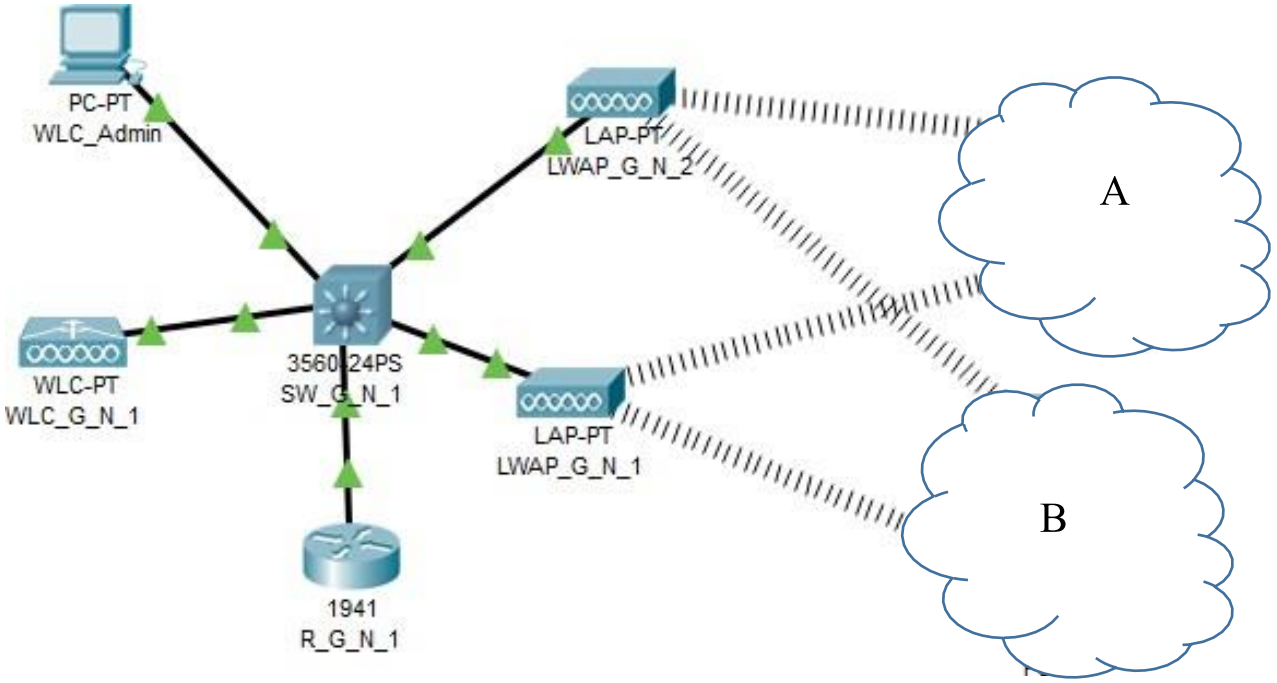

Рисунок 4.20 – Проєкт мережі Wireless Lan Controller

1. У середовищі програмного симулятора/емулятора створити проєкт мережі (рис. 4.20). 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.
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	Номер 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 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 контролер?

Лабораторна робота № 5. Налагодження та дослідження роботи CISCO MERAKI

Мета роботи: ознайомитися з особливостями функціонування пристроїв Cisco Meraki mx-65x; отримати практичні навички налагадження та моніторингу роботи пристроїв в мережі, побудованій на базі обладнання Cisco; дослідити процес роботи та процеси передачі даних у побудованій мережі.

Теоретичні відомості

Cisco Meraki — це IT-компанія з хмарним управлінням, штаб-квартира якого розташована в Сан-Франциско, штат Каліфорнія. Їх рішення включають в себе бездротову передачу, комутацію, безпеку, управління мобільністю підприємства (EMM), комунікації та камери безпеки, усі централізовано керовані з Інтернету. Meraki був придбаний компанією Cisco Systems у грудні 2012 року.

Meraki заснували Санджит Бісвас і Джон Бікет та Ханс Робертсон. Компанія була заснована частково на проєкті MIT Roofnet, експериментальної мережі 802.11b/g, розробленої Лабораторією комп'ютерних наук та штучного інтелекту в Інституті технологій Массачусетса.

Meraki був профінансований компанією Google та Sequoia Capital. Організація була розташована в Маунтін-В'ю, штат Каліфорнія, у 2006 році, а потім переїхала до Сан-Франциско.

18 листопада 2012 року компанія Cisco Systems оголосила, що придбає Meraki приблизно 1,2 мільярда доларів.

За шість років після придбання Meraki нараховує 1590 співробітників Cisco, які працюють в усьому світі. Підрозділ має близько 250 000 унікальних клієнтів і більше 3,5 мільйонів пристроїв в Інтернеті.

Продукти розроблені Meraki слідують принциту plug-and-play, з простим апаратним забезпеченням та легким для розуміння програмним інтерфейсом,

який означає, що компанія з малим та середнім розміром може створити бездротову мережу, не наймаючи людей з особливою підготовкою та навичками, на рисунку 5.1 зображено зовнішній вигляд пристроїв.

Рисунок 5.1 – Лінійка пристроїв Cisco Meraki

Продукція, розроблена Meraki також поділяється на різні серії, відносно їх призначення:

MR серія

Серія Meraki MR є першою в світі лінійкою точок доступу WLAN, керованої через хмару. Розроблені для складних бізнес-середовищ, точки доступу MR використовують вдосконалені технології 802.11ac та 802.11n, включаючи MIMO, формування променя та зв'язування каналів для забезпечення пропускної здатності та надійного покриття, необхідного для вимогливих бізнес-додатків.

MS серія

Cisco Meraki MS є першою в галузі комутатором керованого доступу та агрегації, що поєднує переваги централізованого керування у хмарі з потужною, надійною платформою доступу.

Завдяки керуванню через хмару, тисячі портів комутатора можуть бути налаштовані та відстежені миттєво через Інтернет. Надавати віддалені сайти без IT-об'єктів на місці, розгортати зміни в конфігурації в мережі, а також легко

керувати кампусом і розподіленими мережами без навчання та спеціалізованого персоналу.

MX серія

Meraki MX — це корпоративний пристрій безпеки та SD-WAN, призначений для розподілених розгортань, які потребують віддаленого адміністрування. Він ідеально підходить для мережевих адміністраторів, які вимагають як простоти розгортання, так і сучасного набору функцій.

MC серія

Meraki MC є кінцевою точкою співпраці класів підприємств, розробленої для зручності управління та віддаленого адміністрування. Він ідеально підходить для адміністраторів, які хочуть швидко і легко розгортати та керувати розподіленими телефонними системами.

MV серія

Сімейство продуктів Cisco Meraki MV — це лінійка обладнання, призначеного для встановлення всередині приміщень або ззовні, які є надзвичайно простими для розгортання та налаштування, завдяки їхній інтеграції в інформаційну панель Meraki Dashboard та використання хмарних зон. Сімейство MV усуває складні та дорогі апаратні засоби, необхідні для традиційних рішень, тим самим усуваючи обмеження, які зазвичай присутні при розгортанні систем відеоспостереження.

Також у Meraki є рішення для керування пристроями та мережами під назвою Systems Manager. Одним з найбільших переваг Systems Manager є можливість реєструвати, керувати та контролювати багато різних типів пристроїв. Оскільки кожна операційна система має унікальний набір функцій MDM, важливо ознайомитися з відповідною документацією пристроїв якими ви плануєте керувати.

Для налаштування цих служб рекомендується використовувати спільний або організаційний ідентифікатор Apple, замість персонального ідентифікатора Apple, оскільки інші користувачі також можуть запитувати доступ до облікового запису, щоб відновити ці служби в майбутньому.

Systems Manager включає в себе такі технології:

- Mobile Device Management (MDM),
- Mobile Application Management (MAM),
- Mobile Content Management (MCM),
- Mobile Identity Management (MIM).

Нижче наведено приклади використання цих технологій в цьому рішенні:

- Незареєстровані кінцеві точки доступу до мережі в приміщенні будуть переадресовані на сторінку реєстрації у хмарі Cisco Meraki EMM для реєстрації на основі ролі користувача, типу пристрою тощо. Крім того, Meraki також можна налаштувати для роботи з віддаленими пристроями через, наприклад, AnyConnect (VPN), Jabber (колаборація) тощо, так що користувач має безпечний доступ до корпоративних ресурсів, коли він перебуває поза приміщенням.
- Невідповідним кінцевим точкам буде наданий обмежений доступ на основі стану відповідності.
- Періодично перевіряє відповідність з хмарним сервером Cisco Meraki EMM.
- Можливість для адміністраторів ISE запитувати віддалені дії на пристрої через хмару Cisco Meraki EMM.
- Можливість кінцевого користувача використовувати порт ISE My Devices для керування особистими пристроями, наприклад, повне видалення, корпоративне видалення та блокування PIN-коду.

Для відалленого моніторингу мережі існує продукт Meraki Insight розроблений таким чином, щоб забезпечити клієнтам Meraki простий спосіб контролю продуктивності веб-додатків у їхніх мережах і легко визначити, чи, ймовірно, проблеми викликані Мережею або Програмою. Ця інформація представлена у вигляді легко зрозумілих графіків та діаграм, які чітко показують, чи є проблеми продуктивності в локальній мережі або якщо проблеми з продуктивністю є наслідком чогось на рівні програми або WAN.

Існує два основних типи адміністраторів інформаційної панелі: організація

та мережа.

Адміністратори організації мають повний доступ до своєї організації та всіх її мереж. Цей тип облікового запису еквівалентно адміністратору root або домену, тому важливо фіксувати, хто має такий рівень доступу. Нижче наведено перелік найкращих практик стосовно цих облікових записів.

Мережеві адміністратори мають доступ до окремих мереж та їх пристроїв. Ці користувачі можуть мати повний або обмежений контроль над своєю конфігурацією мережі, але не мають доступу до інформації на рівні організації (ліцензування, інвентаризації пристроїв тощо).

Типи дозволів мережі

Гістьовий доступ: користувач має змогу побачити список користувачів автентифікації Meraki, додавати користувачів, оновлювати існуючих користувачів та авторизувати або обмежувати користувачів за ідентифікатором SSID або клієнтом VPN.

Монітор: користувач може переглядати лише розділ "Монітор" на панелі інструментів, і ніяких змін не можна зробити.

Лише для читання: користувач має доступ до більшості аспектів мережі, включаючи розділ Налаштування, але жодних змін не можна зробити.

Повний : користувач має доступ, щоб переглянути всі аспекти мережі та вносити до неї будь-які зміни.

На вкладці Connection можна переглянути параметри IP, MAC-адреси підключених клієнтів та стан самого пристрою (рис. 5.2).

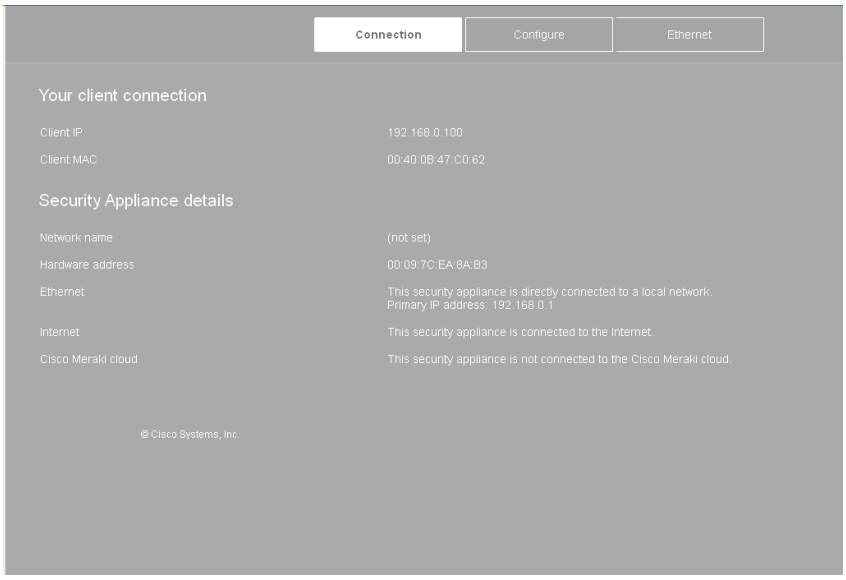

Рисунок 5.2 − Вкладка connection пристрою meraki-mx65x

На вкладці Configure налаштовуються параметри з’єднання з мережею Internet за допомогою статичної IP-адресації або за DHCP чи PPPoE (рис. 5.2-5.3).

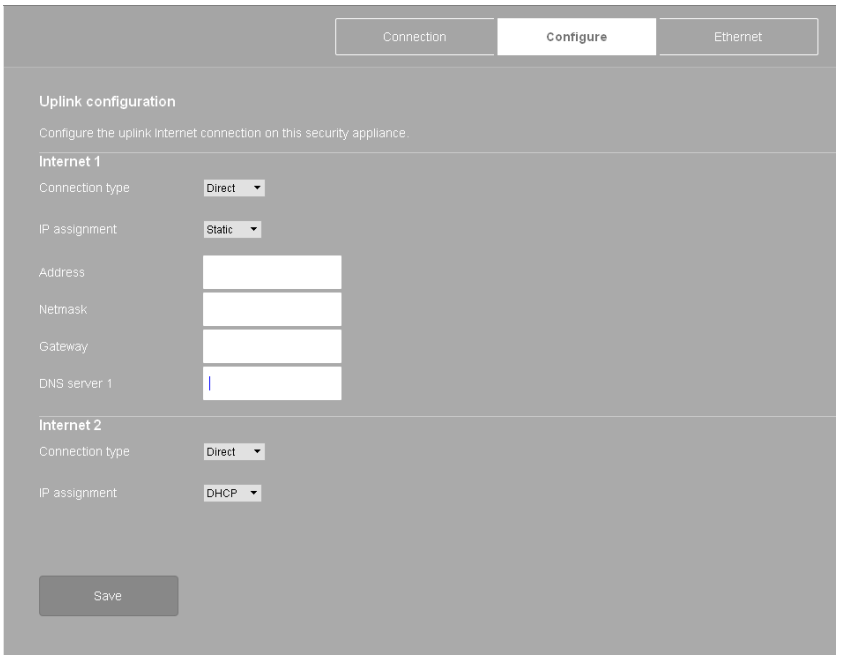

Рисунок 5.3 − Налаштування підключення зі статичною адресацією та DHCP configure пристрою meraki-mx65x

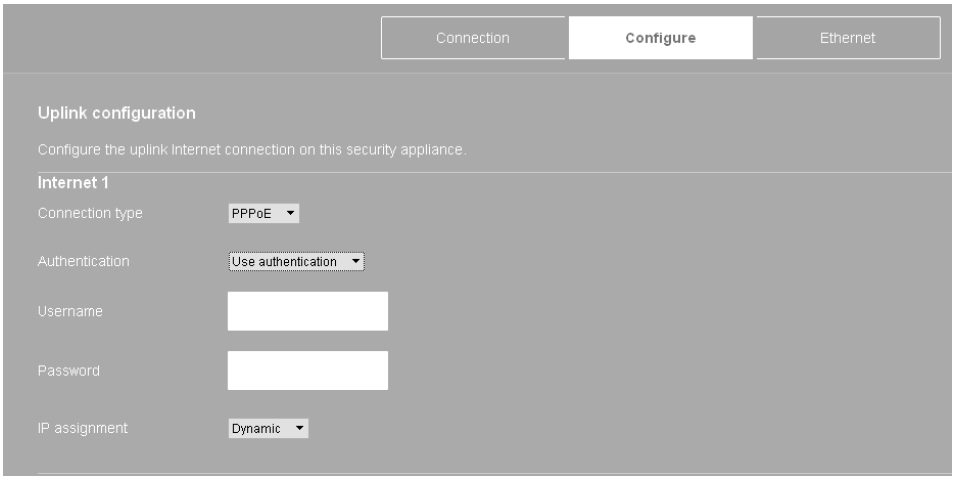

Рисунок 5.4 − Налаштування підключення через PPPoE пристрою meraki-mx65x

На вкладці Ethernet налаштовуються параметри режиму роботи інтерфейсів пристрою, зокрема і їх вимкнення, як показано на рис. 5.5.

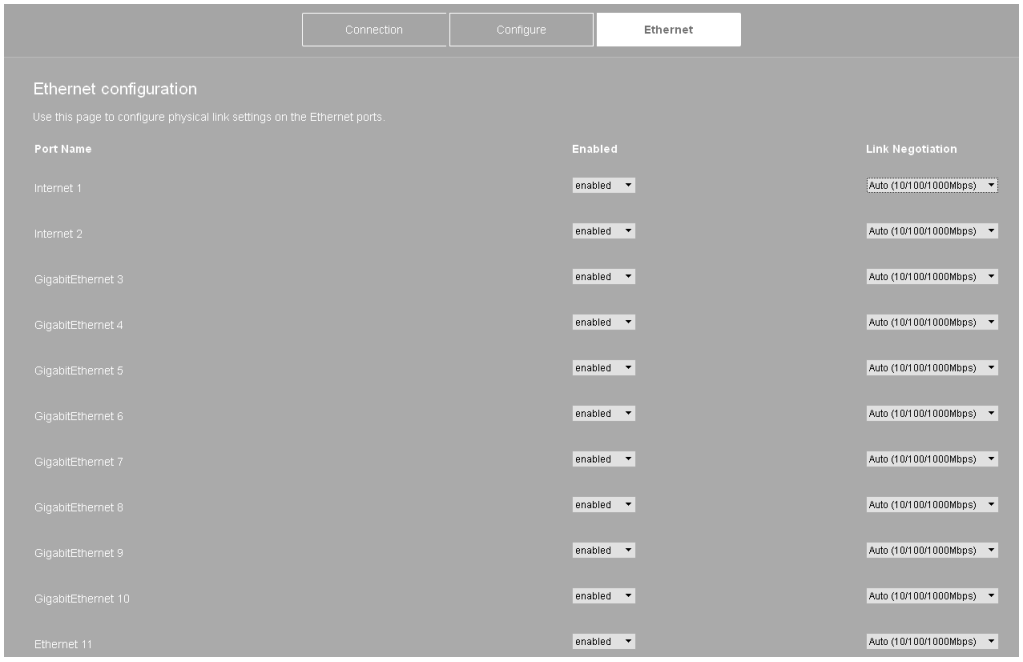

Рисунок 5.5 − Вкладка ethernet пристрою meraki-mx65x

Для решти налаштувань використовується сервер Meraki або Cisco Cloud. Вкладка *Network-wide* web-сторінки Cisco Server (рис. 5.6) дозволяє переглянути та додати користувачів, організації та мережі.

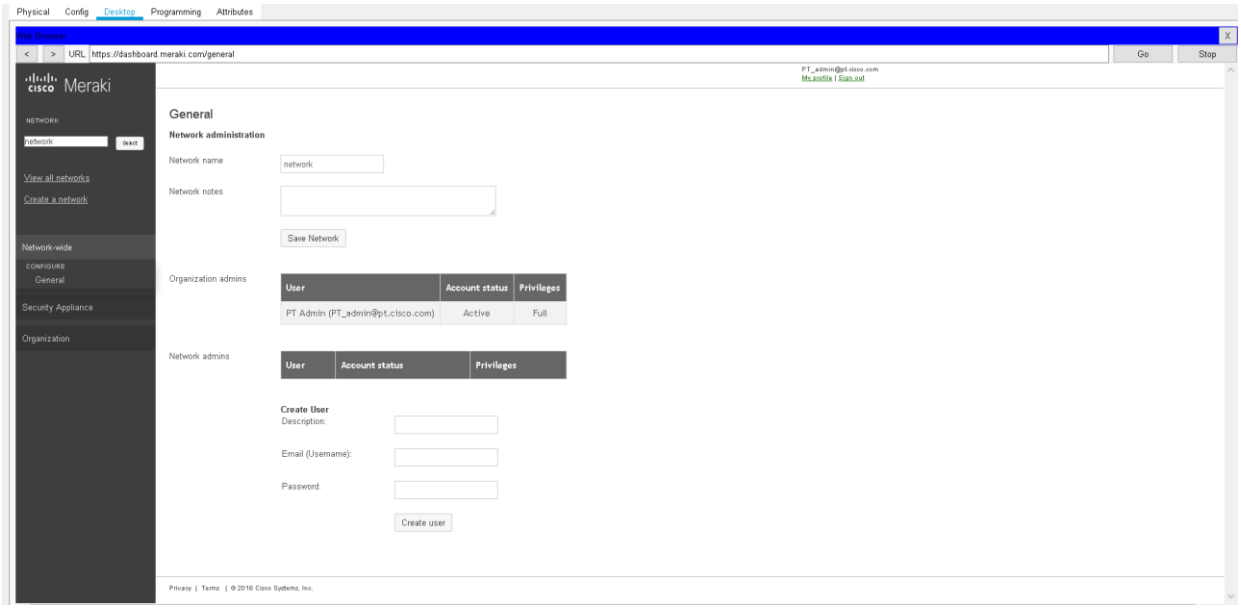

Рисунок 5.6 − Сторінка network-wide сервера meraki

Вкладка *Secure Appliance* web-сторінки Cisco Server в підрозділі *Appliance Status* дозволяє переглянути підключення до портів пристрою (рис. 5.7), параметри підключення до мережі Інтернет (рис. 5.8) та налаштування DHCP-сервера (рис. 5.9).

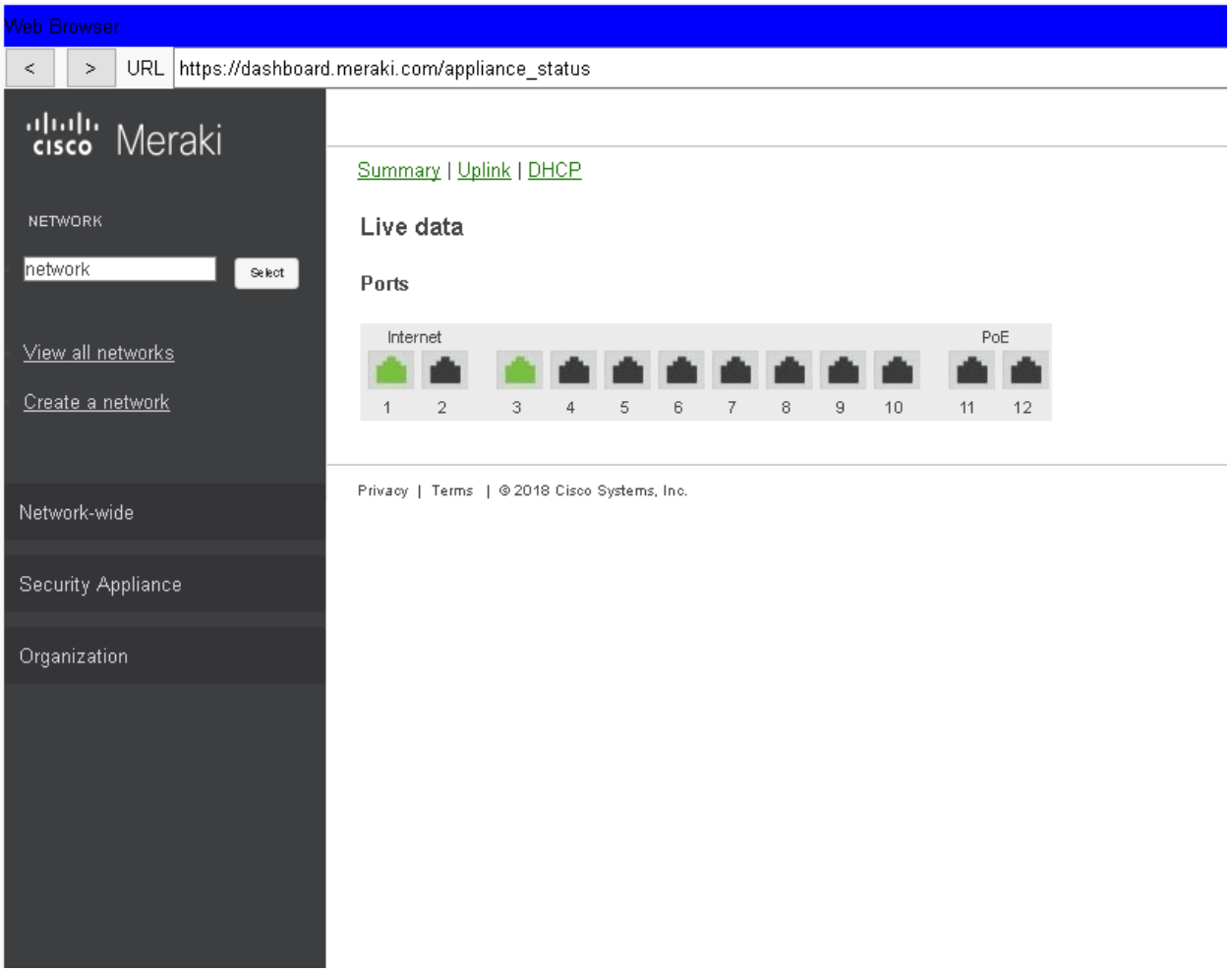

Рисунок 5.7 − Статус підключення портів пристрою meraki-mx65x на сервері meraki

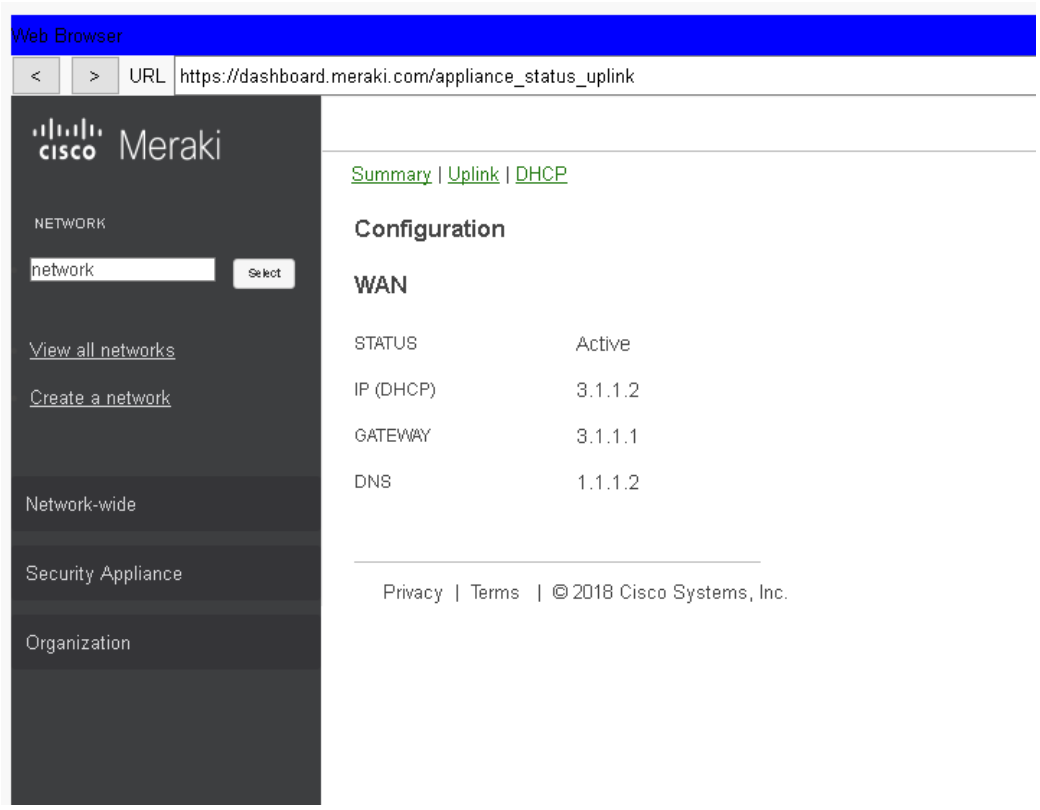

Рисунок 5.8 − Статус підключення до Інтернету пристрою meraki-mx65x на сервері meraki

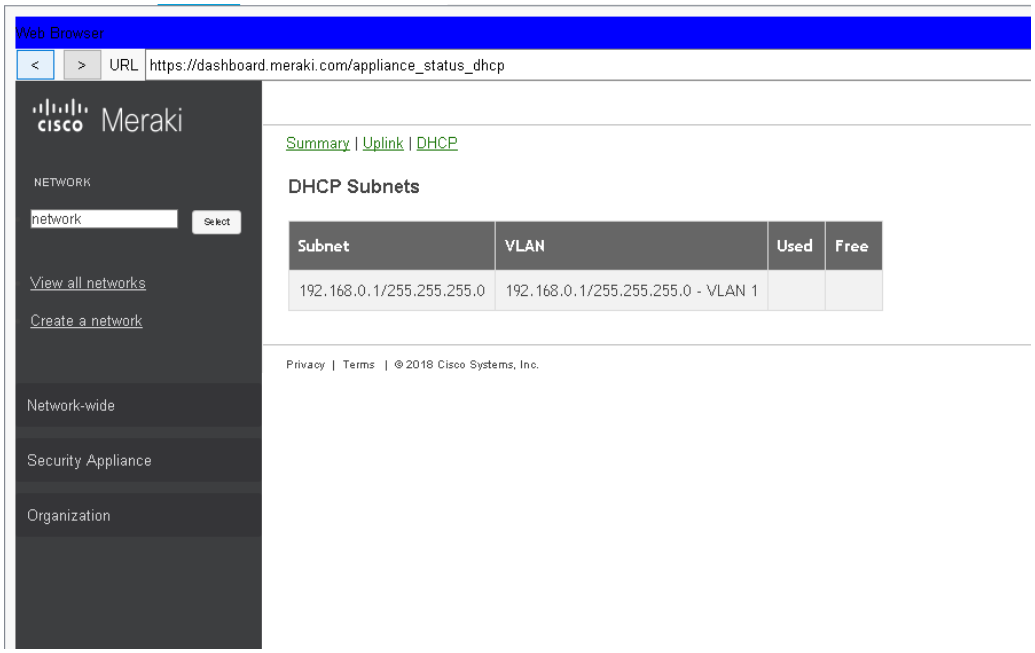

Рисунок 5.9 − Параметри DHCP-сервера пристрою meraki-mx65x на сервері meraki

Підрозділ *Addressing & VLANs* дозволяє налаштувати віртуальні локальні мережі VLAN, тунельні підключення VPN або технологію NAT (рис. 5.10).

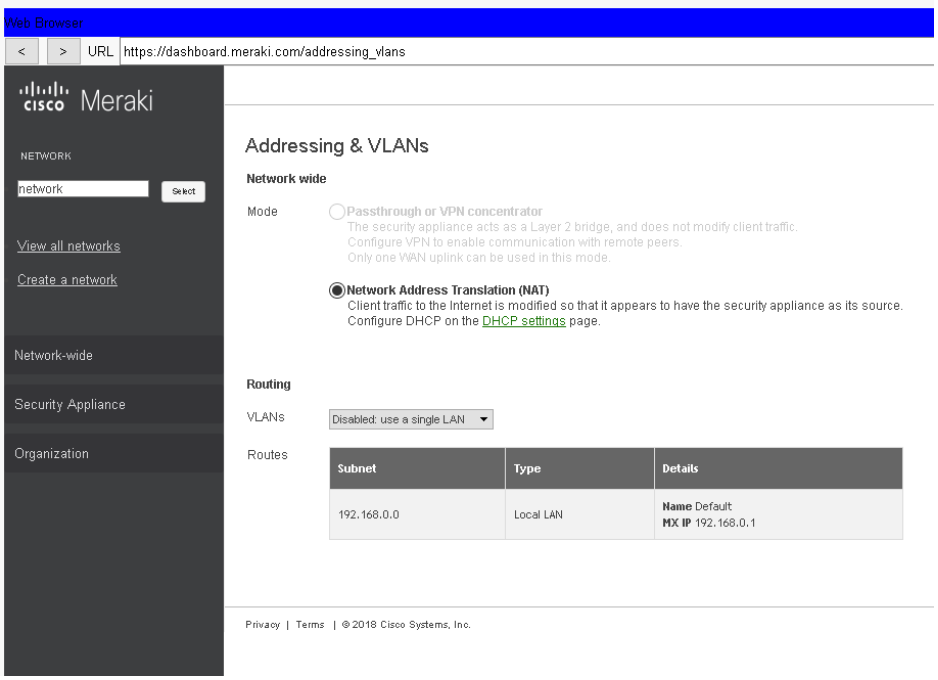

Рисунок 5.10 − Вкладка Addressing & VLANs сервера meraki

Підрозділ *Wireless settings* дозволяє увімкнути або вимкнути бездротову мережу Wi-Fi, налаштувати параметри захисту мережі та приховати SSID (рис. 5.11).

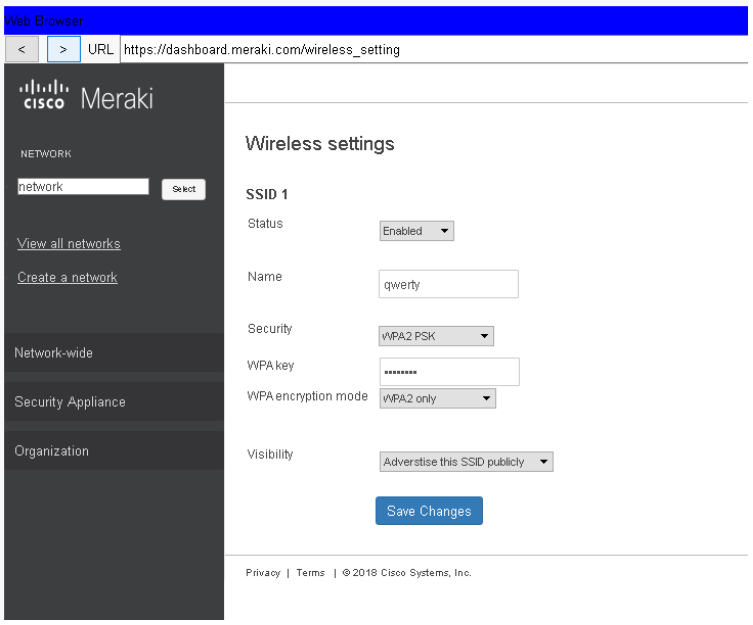

Рисунок 5.11 - Вкладка Wireless settings сервера meraki

Підрозділ *DHCP* дозволяє увімкнути або вимкнути DHCP-сервер для LAN, налаштувати час оренди адреси та параметри адресації (рис. 5.12).

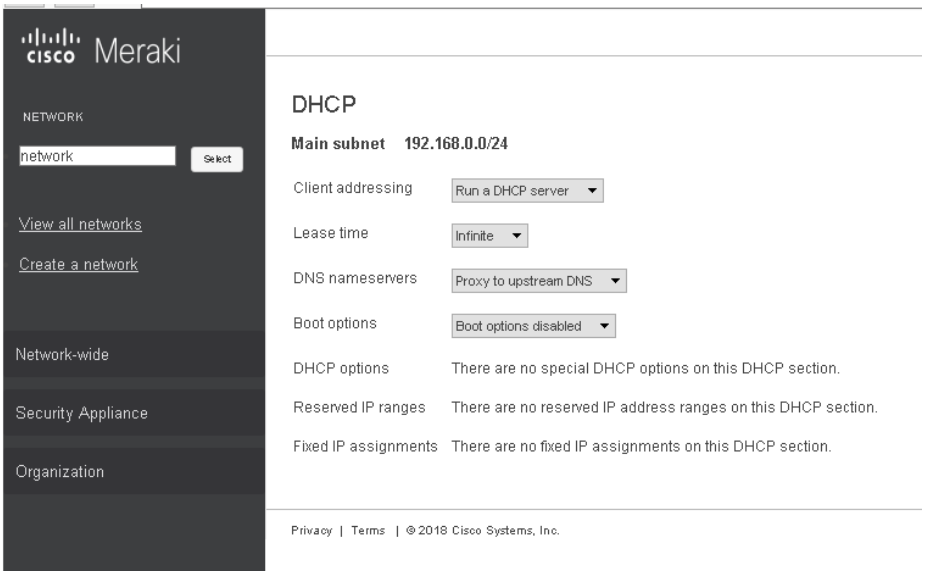

Рисунок 5.12 − Вкладка DHCP сервера meraki

Підрозділ *Firewall* дозволяє блокувати трафік за протоколами UDP, TCP, ICMP залежно від адреси та порту отримувача і відправника, як зображено на рис. 5.13.

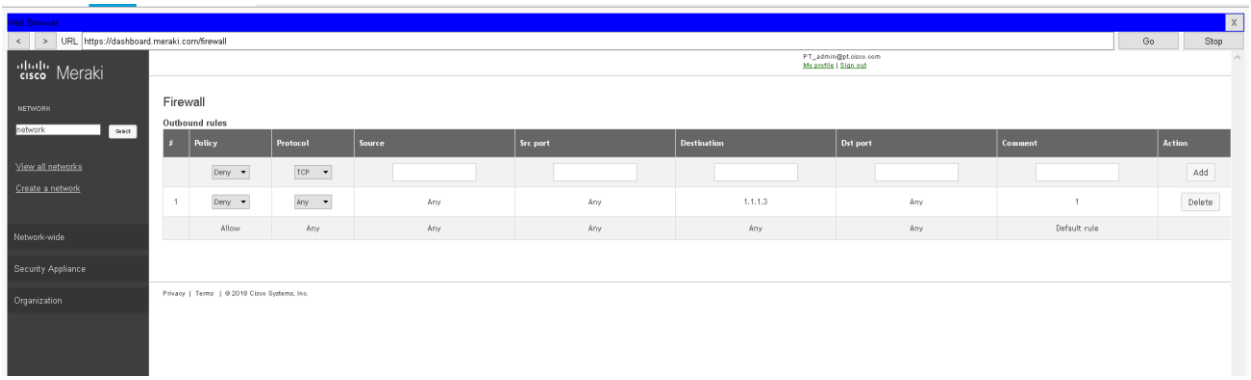

Рисунок 5.13 − Вкладка Firewall сервера meraki

Модельний приклад налагодження функціонування Meraki на обладнанні Cisco

Розглянемо порядок налагодження Secure Appliance meraki mx-65x у мережі, схема якої наведена на рис. 5.14. Для даної мережі для з'єднання пристроїв використано дані табл. 1, 2 .

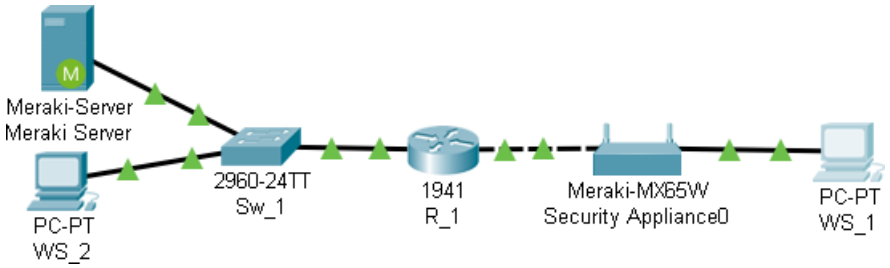

Рисунок 5.14 − Схема мережі модельного прикладу

Таблиця 1

Параметри інтерфейсів для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Комутатор SW_1	Fa 0/1	Маршрутизатор R_1	Gig 0/0
	Fa 0/2	Робоча станція WS_2	Fa 0
	Fa 0/3	Сервер Meraki Server	Fa 0
Маршрутизатор R_1	Gig 0/0	Комутатор SW_1	Fa 0/1
	Gig 0/1	Secure Appliance	internet 1
Робоча станція WS_1	Gig 0	Маршрутизатор R_1_3_1	Gig 3
Робоча станція WS_2	Fa 0	Комутатор SW_1	Fa 0/2
Сервер Meraki Server	Fa 0	Комутатор SW_1	Fa 0/3
Secure Appliance	internet 1	Маршрутизатор R_1_3_3	Gig 0/1
	Gig 3	Робоча станція WS_1	Fa 0

Таблиця 2

Схема адресації для прикладу

Мережа/пристрій	Інтерфейс/ мережевий адаптер/шлюз	IP-адреса	Маска	Префікс
Мережа A	-	192.168.0.0	255.255.255.0	/24
Мережа B	-	3.1.1.0	255.255.255.0	/24
Мережа C	-	1.1.1.0	255.255.255.0	/24
Маршрутизатор R_1	Gig 0/0	1.1.1.1	255.255.255.0	/24
	Gig 0/1	3.1.1.1	255.255.255.0	/24
Secure Appliance	internet 1	3.1.1.2	255.255.255.0	/24
	Vlan 1	192.168.0.1	255.255.255.0	/24
Сервер Meraki Server	Мережевий адаптер	1.1.1.2	255.255.255.0	/24
	Шлюз за замовчуванням	1.1.1.1	-	-
	DNS-сервер	127.0.0.1	-	-
Робоча станція WS_1	Мережевий адаптер	DHCP		
	Шлюз за замовчуванням			
	DNS-сервер			
Робоча станція WS_2	Мережевий адаптер	1.1.1.3	255.255.255.0	/24
	Шлюз за замовчуванням	1.1.1.1	-	-
	DNS-сервер	1.1.1.2	-	-

Розглянемо випадок налаштувань зі статичною IP-адресацією та базовим налагодженням параметрів бездротової мережі.

Сценарій налагодження маршрутизатора R_1 наведено нижче:

…
Router(config)#hostname R_1
R_1(config)#interface gig0/0
R_1(config-if)#ip address 3.1.1.1 255.255.255.0
R_1(config-if)#no shutdown
R_1(config-if)#interface gig0/1
R_1(config-if)#ip address 1.1.1.1 255.255.255.0
R_1(config-if)#no shutdown
…

Розглянемо порядок налагодження ***Security Appliance.***

Додайте пристрій Meraki до Вашого проєкту мережі та підключіть блок живлення в налаштуваннях “Physical”. Додайте також робочу станцію та замініть в ній модуль на бездротовий, після чого підключіться до бездротової мережі пристрою Meraki, вона повинна мати SSID “**Default**” та підключатись без пароля – це необхідно для першого налаштування Meraki.

Далі потрібно на робочій станції відкрити Web-браузер та ввести IP-адресу пристрою Meraki – **192.168.0.1**. **По замовчуванню для входу використовується серійний номер в якості логіну без паролю**. На вкладці Configure налаштовуються параметри IP-адресації інтерфейсу підключення до інтернету. Для збереження налаштувань використовується кнопка Save (рис. 5.15-5.16).

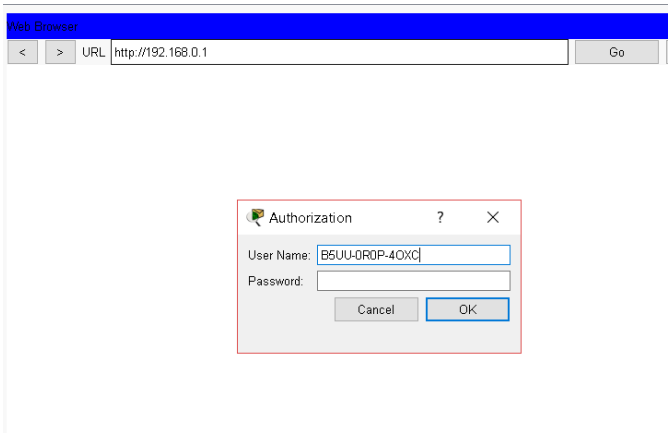

Рисунок 5.15 − Вікно входу на web-сторінку пристрою meraki-mx65x

Після успішного входу до Meraki, необхідно перейти до пункту «Configure», та заповнити налаштування інтерфейсів відповідно до параметрів вашої мережі, як показано на рис. 5.16.

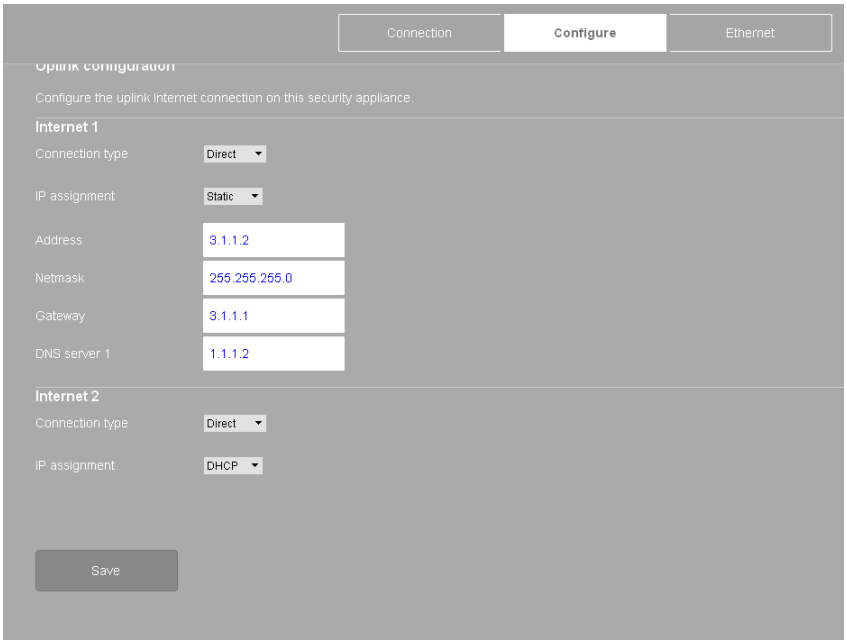

Рисунок 5.16 − Налаштування IP-адресації для підключення до мережі Інтернет

Розглянемо порядок налагодження ***Meraki Server.***

Для переходу на сторінку налагодження використовується посилання https://dashboard.meraki.com, далі потрібно створити користувача для адміністрування системи, як показано на рис. 5.17.

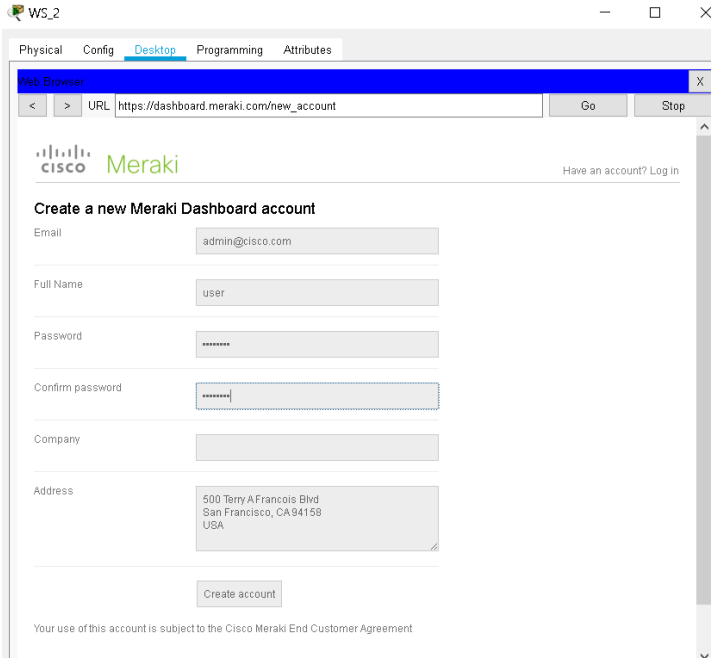

Рисунок 5.17 – Вікно створення нового користувача на сервері meraki

Для створення мережі потрібно перейти на вкладку *Create network*, ввести назву нової мережі та натиснути кнопку Create network (рис. 5.18).

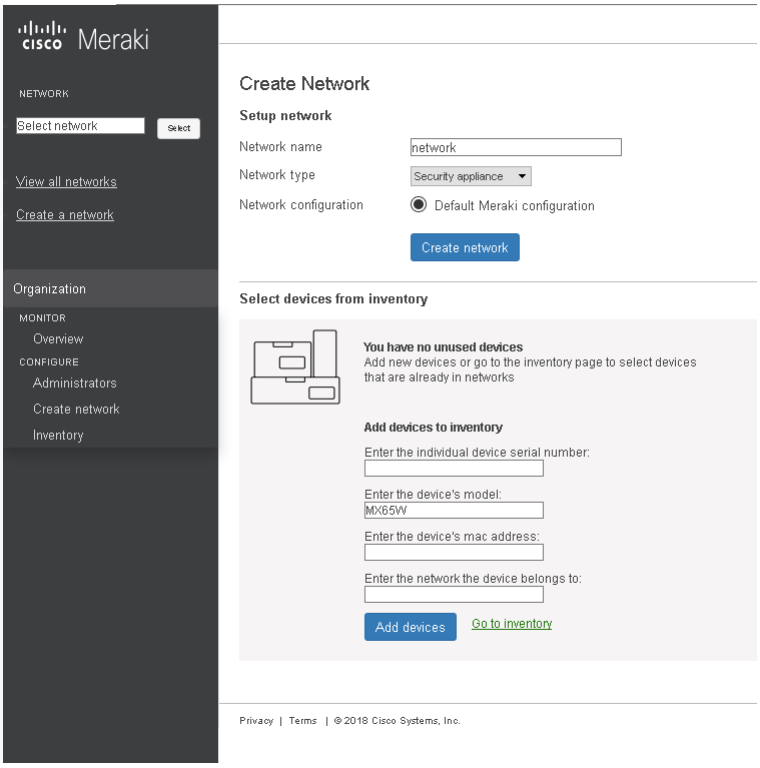

Рисунок 5.18 – Створення нової мережі

Щоб додати пристрій для адміністрування на вкладці *Create network*, потрібно ввести серійний номер пристрою, що додається, в поле ***Enter the individual device serial number***, MAC-адресу пристрою в поле ***Enter the device's mac address***, назву мережі, до якої додається пристрій в поле ***Enter the network the device belongs to*** та натиснути кнопку *Add devices* (рис. 5.19).

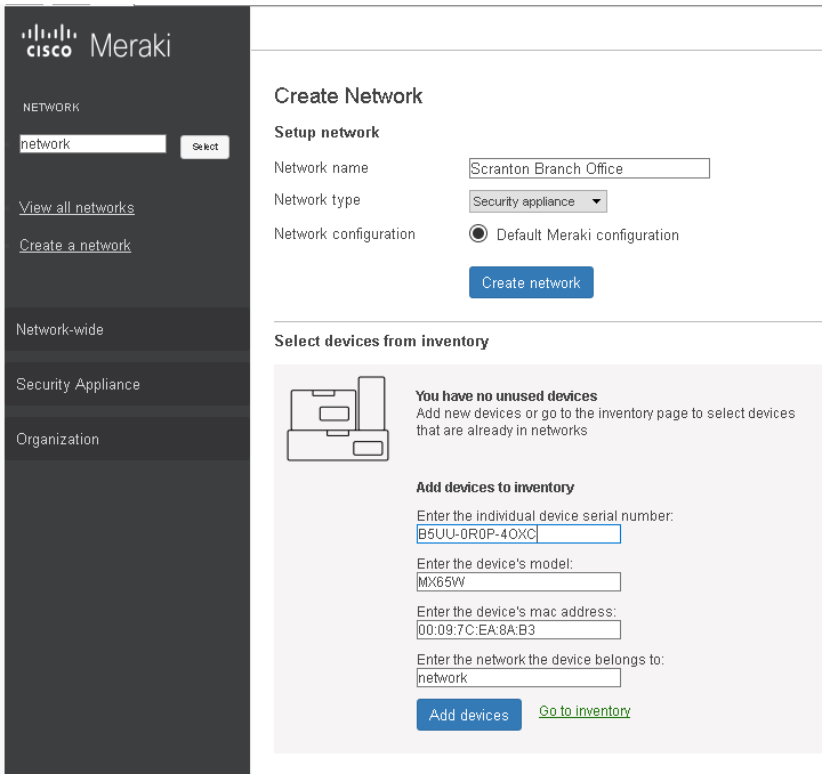

Рисунок 5.19 – Додавання пристрою meraki-mx65x до створеної мережі

Для налаштування параметрів бездротової мережі потрібно на вкладці *Security Appliance* перейти на вкладку *Wireless settings* та ввести параметри SSID, методу захисту з’єднання і натиснути кнопку *Save Changes* (рис. 5.20). На цьому налаштування системи можна вважати завершеним.

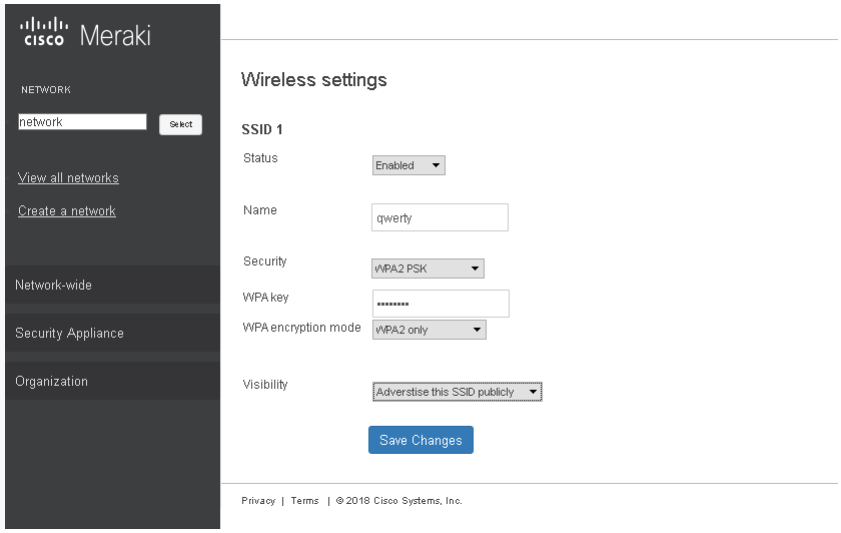

Рисунок 5.20 − Налаштування параметрів мережі Wi-Fi

Завдання на лабораторну роботу

1. У середовищі програмного симулятора/емулятора створити проєкт мережі (рис. 5.21). При побудові звернути увагу на вибір моделей пристроїв, мережевих модулів та адаптерів, а також мережевих з'єднань. Канали підключення кінцевих вузлів довільні. Для побудованої мережі заповнити описову таблицю.

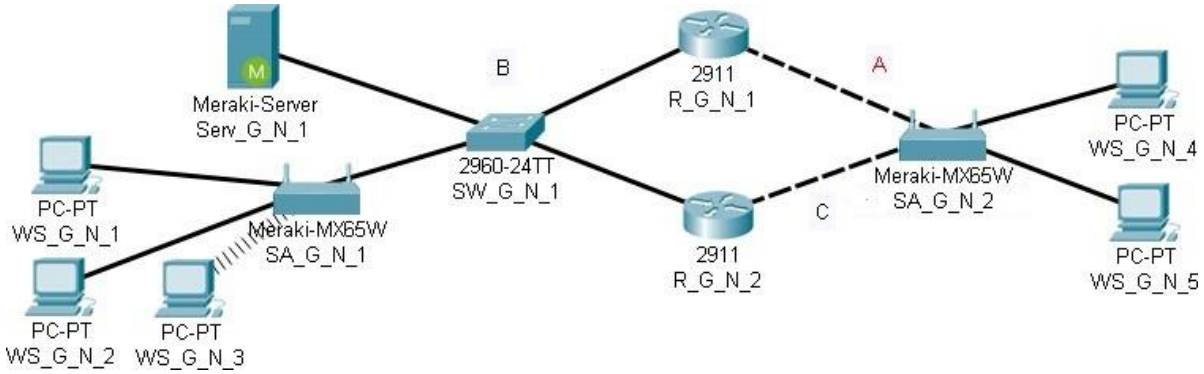

Рисунок 5.21 − Топологія мережі

2. Розробити схему адресації пристроїв мережі. Для решти мереж використовувати дані табл. 3, 4. Результати навести у вигляді таблиці, яка аналогічна табл. 2.

Таблиця 3

Дані для адресації підмереж

№ варіанту	Мережа А		Мережа В		Мережа С	
	IP-адреса	префікс	IP-адреса	префікс	IP-адреса	префікс
1	193.G.N.0	/30	194.G.N.128	/25	195.G.N.0	/30
2	193.G.N.4	/30	194.G.N.64	/26	195.G.N.4	/30
3	193.G.N.8	/30	194.G.N.192	/26	195.G.N.8	/30
4	193.G.N.12	/30	194.G.N.32	/27	195.G.N.12	/30
5	193.G.N.16	/30	194.G.N.96	/27	195.G.N.16	/30
6	193.G.N.20	/30	194.G.N.160	/27	195.G.N.20	/30
7	193.G.N.24	/30	194.G.N.224	/27	195.G.N.24	/30
8	193.G.N.28	/30	194.G.N.16	/28	195.G.N.28	/30
9	193.G.N.32	/30	194.G.N.48	/28	195.G.N.32	/30
10	193.G.N.36	/30	194.G.N.80	/28	195.G.N.36	/30
11	193.G.N.40	/30	194.G.N.112	/28	195.G.N.40	/30
12	193.G.N.44	/30	194.G.N.144	/28	195.G.N.44	/30
13	193.G.N.48	/30	194.G.N.176	/28	195.G.N.48	/30
14	193.G.N.52	/30	194.G.N.208	/28	195.G.N.52	/30
15	193.G.N.56	/30	194.G.N.240	/28	195.G.N.56	/30
16	193.G.N.60	/30	194.G.N.128	/25	195.G.N.60	/30
17	193.G.N.64	/30	194.G.N.64	/26	195.G.N.64	/30
18	193.G.N.68	/30	194.G.N.192	/26	195.G.N.68	/30
19	193.G.N.72	/30	194.G.N.32	/27	195.G.N.72	/30
20	193.G.N.76	/30	194.G.N.96	/27	195.G.N.76	/30
21	193.G.N.80	/30	194.G.N.160	/27	195.G.N.80	/30
22	193.G.N.84	/30	194.G.N.224	/27	195.G.N.84	/30
23	193.G.N.88	/30	194.G.N.16	/28	195.G.N.88	/30

Продовження табл. 3

24	193.G.N.92	/30	194.G.N.48	/28	195.G.N.92	/30
25	193.G.N.96	/30	194.G.N.80	/28	195.G.N.96	/30
26	193.G.N.4	/30	194.G.N.112	/28	195.G.N.4	/30
27	193.G.N.24	/30	194.G.N.144	/28	195.G.N.24	/30
28	193.G.N.44	/30	194.G.N.176	/28	195.G.N.44	/30
29	193.G.N.64	/30	194.G.N.208	/28	195.G.N.64	/30
30	193.G.N.84	/30	194.G.N.240	/28	195.G.N.84	/30

3. Провести базове налагодження пристроїв, інтерфейсів та каналів зв’язку.

4. Провести налагодження параметрів IP-адресації пристроїв мережі у відповідності до даних, які отримані у п. 2. Провести налагодження протоколу DHCP для мережі B та протоколу PPPoE для мережі C. Перевірити наявність зв’язку між сусідніми парами пристроїв мережі.

5. Провести налагодження підключень до мережі для пристрою SA_G_N_1 за допомого протоколу DHCP, для пристрою SA_G_N_2 за допомогою статичної адресації та протоколу PPPoE.

6. Провести налагодження параметрів мереж та пристроїв на сервері. Налаштувати параметри бездротових мереж.

7. Перевірити стан пристроїв та підключень на сервері, у разі наявності проблем виправити їх.

Контрольні питання:

1. Назвіть відомі вам серії пристроїв Cisco Meraki та їх основне призначення
2. Опишіть типи дозволів мережі які використовуються у мережах Meraki.
3. Опишіть процес створення мережі в dashboard.
4. Дайте визначення типів адміністраторів інформаційної панелі.
5. В чому основний принцип розробки Meraki?

Лабораторна робота №6. Налагодження бездротової SOHO-мережі на обладнанні MikroTik.

Мета заняття: навчитися налаштовувати SOHO бездротові мережі; підключати точки доступу hAP; налагодити захист бездротової мережі; налаштувати та дослідити IP-адресацію в мережі.

Теоретичні відомості

Загальні відомості про виробника

MikroTik − латвійській виробник мережевого устаткування. Компанія розробляє та пропонує Ethernet та бездротове мережеве обладнання, зокрема маршрутизатори, мережеві комутатори, точки доступу, а також програмне забезпечення - операційні системи, RouterOS, та допоміжні продукти (рис. 6.1). Компанію було засновано у 1996 році з метою продажу обладнання на ринках, які розвиваються.

Рисунок 6.1 – Продукція компанії MikroTik

RouterOS − мережева операційна система на базі Linux, розроблена латвійською компанією MikroTik та призначена для встановлення на маршрутизаторах RouterBoard виробництва цієї ж однойменної фірми. Існує можлівість встановлення даної системи на ПК, що дозволяє наділити пристрій деякими функціями маршрутизатора ("перетворення" в брендмауер, VPN - сервер/клієнт, QoS, точку доступу тощо). Система також може служити в якості Captive - порталу на основі бездротового доступу. RouterOS підтримує безліч сервісів та протоколів, які можуть бути використані середніми або великими провайдерами - таких, як OSPF, BGP, VPLS/MPLS. RouterOS забезпечує підтримку практично всіх мережевих інтерфейсів на ядрі Linux та надає системному адміністратору графічний інтерфейс (WinBox) для наочної та швидкої конфігурації пристрою.

Налаштування маршрутизатора hAP AC^2

Оновлення RouterOS

Перше, що необхідно зробити перед налаштуванням бездротового маршрутизатора hAP AC^2 - це скинути налаштування до заводських та оновити версію Router OS.

Для оновлення версії RouterOS використаємо програму WinBox останньої версії з офіційного сайту MikroTik. Для Windows: https://mikrotik.com/download

Запускаємо WinBox і знаходимо в мережі роутер з IP 192.168.88.1 (рис. 6.2).

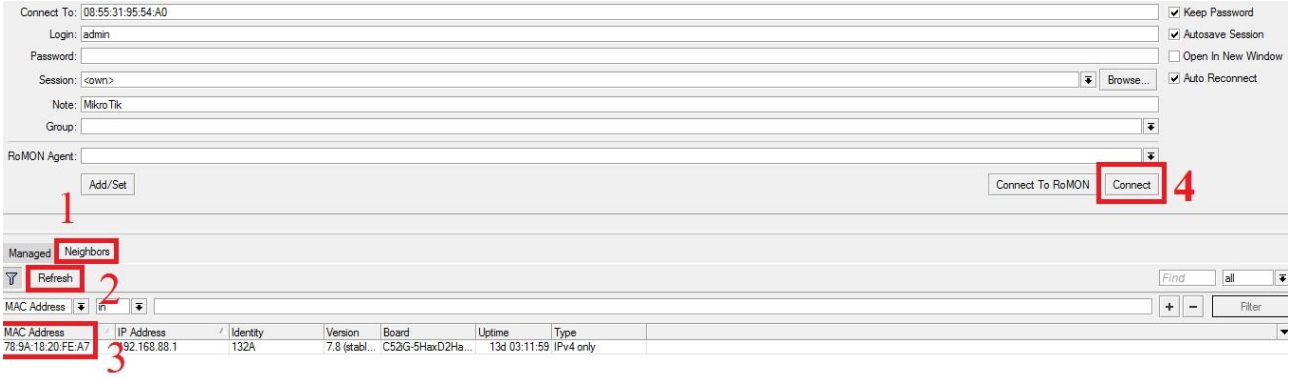

Рисунок 6.2 – Знайдений маршрутизатор у програмі WinBox та підключення до нього

Скидання налаштувань – графічний інтерфейс:

Програма WinBox має можливість скинути налаштування пристрою через відповідне меню: System -> Reset Configuration. Приклад такої операції зображено на рис. 6.3.

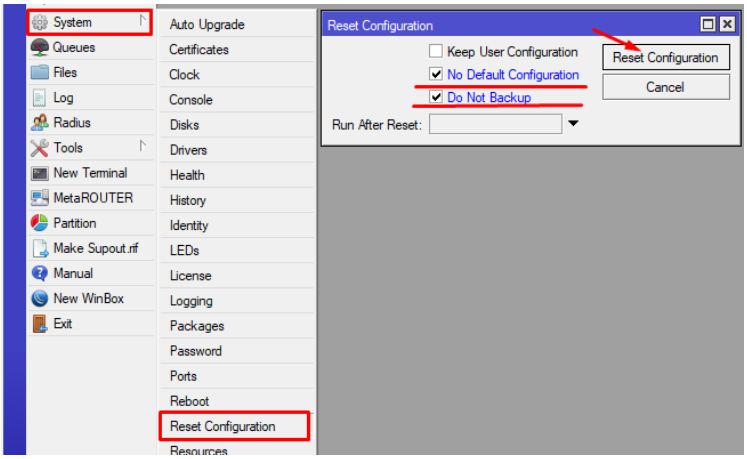

Рисунок 6.3 – Приклад скидання конфігурації маршрутизатора

Скидання налаштувань через консоль:

В консолі пишемо:

/system reset-configuration no-defaults=yes skip-backup=yes

Підтверджуємо скидання налаштувань.

Після цієї процедури, у роутера НЕ буде IP адреси, тому підключаємось за MAC-адресою. Усі налаштуваня будуть відмінені. Процедура скидання буде завершена після автоматичного перезавантаження пристрою.

Налаштування маршрутизатора

1. Налаштуємо фізичні інтерфейси

Меню налаштування інтерфейсів:

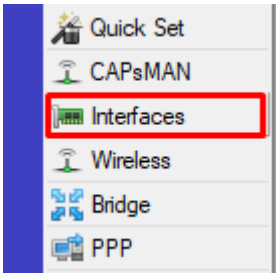

Рисунок 6.4 – Вкладка Interfaces в меню налаштувань

Меню інтерфейсів – **консольна команда**:

/ interface

Всі інтерфейси RJ45 входять в один комутатор (*switch1*), тому нам потрібно відокремити порт для провайдера, і порти для локальних з'єднань. Також є два Wi-Fi інтерфейси та роз'єм SFP. Обираємо інтерфейс *ether1* та перейменовуємо його в WAN, як показано на рис. 6.5, використовуючи графічний інтерфейс WinBox. Приклад зміни назви інтерфейсу через консоль наведено нижче.

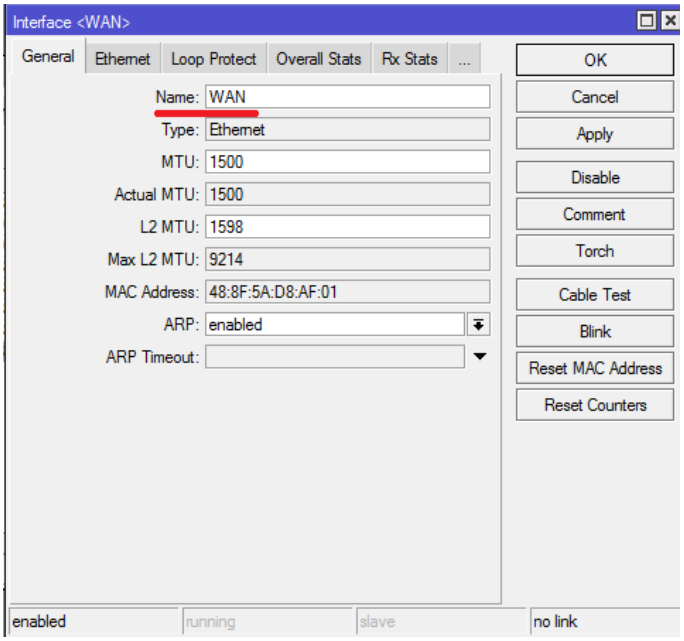

Рисунок 6.5 – Перейменування інтерфейсу

Зміна назви інтерфейсу *ether1* через консоль:

/interface ethernet set [find default-name=ether1] name=WAN

2. Налаштуємо Wi-Fi з'єднання.

У моделі hAP ac^2 присутні два види Wi-Fi. Це 2.4GHz і 5GHz частоти. Відповідно, ми маємо два Wi-Fi інтерфейси - wlan1 та wlan2.

Зайшовши в налаштування кожного, можна визначити, який з них відповідає за певну частоту (рис. 6.6-6.7). Виробник також може використати один і той самий модуль для різних частот.

Рисунок 6.6 – Приклад модуля з робочою частотою 2.4GHz

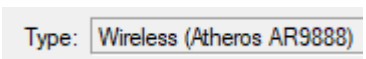

Рисунок 6.7 – Приклад модуля з робочою частотою 5GHz

Через консоль це також можливо визначити за допомогою команди:

/interface wireless print

Для початку налаштуємо профіль авторизації для наших Wi-Fi інтерфейсів (рис. 6.8):

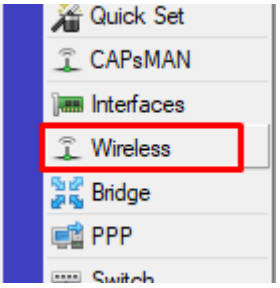

Рисунок 6.8 – Вкладка Wireless в меню налаштувань

Налаштовуємо базовий профіль або додаємо свій (рис. 6.9).

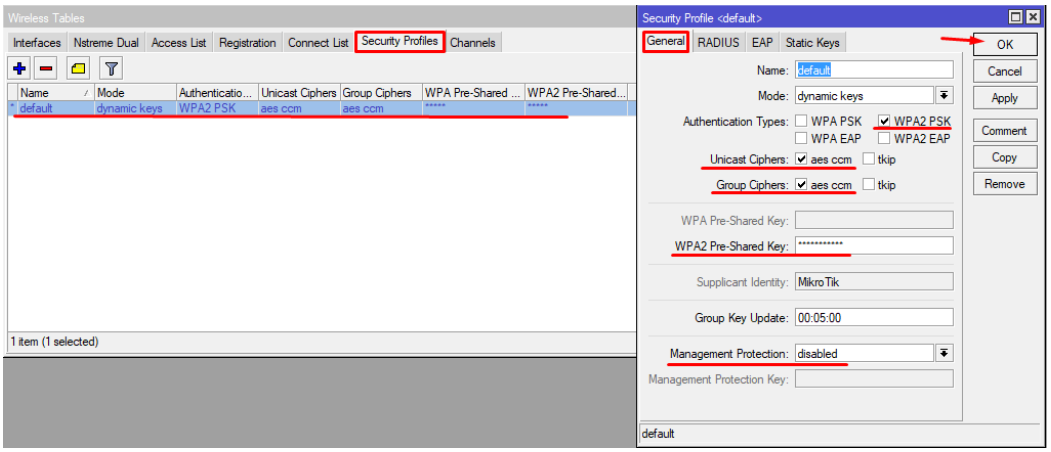

Рисунок 6.9 – Налаштування базового профілю бездротової мережі

Приклад налаштування Wi-Fi через консоль:

Налаштуємо WPA2 Pre-Shared Key - це і буде пароль до Wi-Fi.

/interface wireless security-profiles

set default mode=dynamic-keys authentication-types=wpa2-psk unicast-ciphers=aes-ccm group-ciphers=aes-ccm wpa2-pre-shared-key="12345678" management-protection=disabled

Тепер можна переходити до налаштування самих інтерфейсів Wi-Fi.

Почнемо з інтерфейсу 2.4GHz (рис. 6.10).

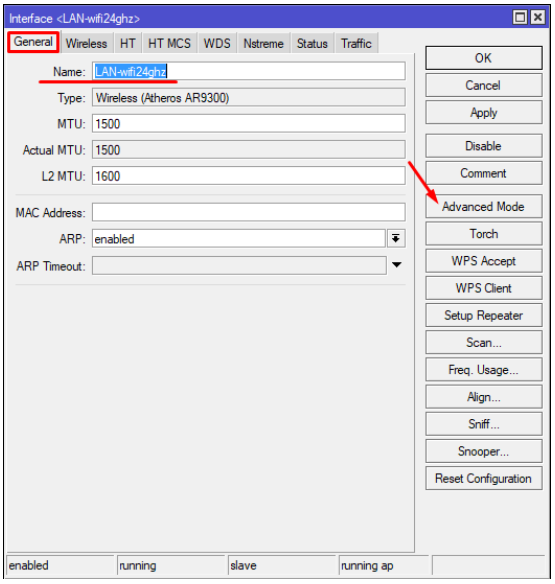

Рисунок 6.10 – Налаштування інтерфейсу 2.4GHz через графічний спосіб

Вкладка General: змінюємо ім’я інтерфейсу — *LAN-wifi24ghz* і активуємо розширений режим (рис. 6.11).

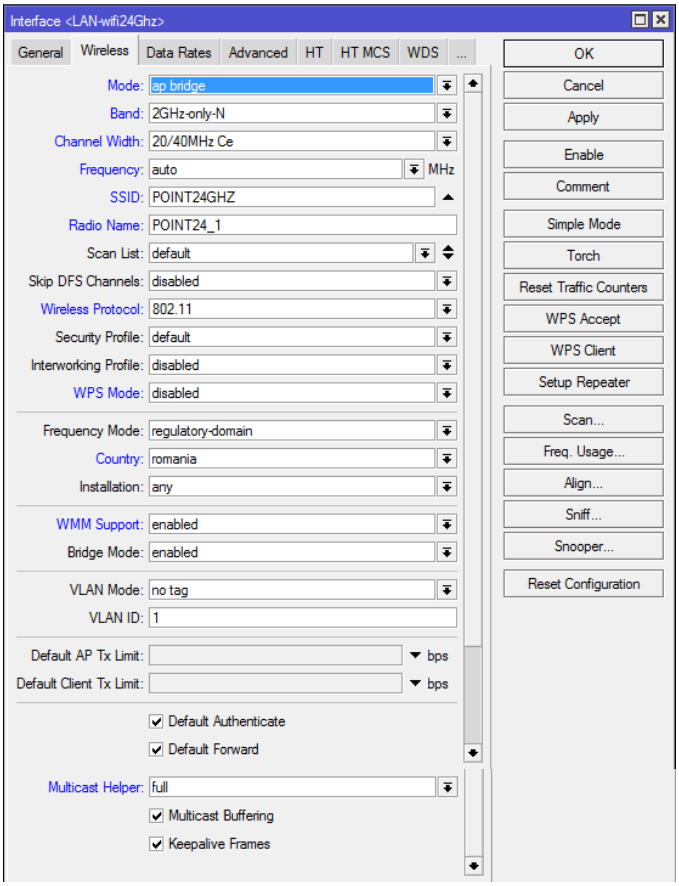

Рисунок 6.11 – Задані налаштування Wireless

Опис параметрів:

Mode - Режим роботи модуля Wi-Fi. Вибираємо режим для роботи як точки

доступу в режимі моста.

Band - Стандарт Wi-Fi з'єднання. Якщо у Вас немає старих ноутбуків або інших пристроїв, які працюють на стандартах b або g, обирайте максимально доступний. Найкраще, якщо у Вас немає пристроїв з b або g, обирайте режим 2GHz-only-N. Навіть якщо у Вас немає таких пристроїв, але Ви залишили режим B/G/N, такі пристрої можуть бути у Ваших сусідів і тоді вся Wi-Fi мережа буде використовувати найнижчий стандарт. Будьте уважні!

Channel Width - Ширина каналу.

Frequency - Робоча частота.

SSID - Ім'я вашої Wi-Fi мережі

Radio Name - Ім'я радіо інтерфейсу, буде відображатись в таблиці реєстрації при підключенні по Wi-Fi до іншого Мікротіку. Необов’язковий параметр.

Wireless Protocol - Обирайте 802.11, тому що інші це протоколи Мікротік.

unspecified - використовувався раніше в RouterOS 3-ої та 4-ої версій.

Security Profile - Обираємо наш профіль шифрування з паролями до Wi-Fi.

WPS Mode - Відключаємо WPS, це покращить безпеку нашої мережі.

Frequency Mode - Частотний режим. Всього є три режими (для конкретної країни, ручне призначення, суперканал). В принципі не важливо, що Ви оберете, головне нічого не порушувати. І щоб не порушувати законодавство потрібно обрати режим, який регулюється країною.

Country - Обмежує доступні діапазони, частоти і максимальну потужність передачі для кожної частоти в залежності від країни.

WMM Support - Вказує, чи слід вносити WMM.

Bridge Mode - Активує режим моста для інтерфейсу.

Default Authenticate - Дозволяє клієнтам автентифікацію за замовчуванням.

Default Forward - Можливість спілкування клієнтів між собою.

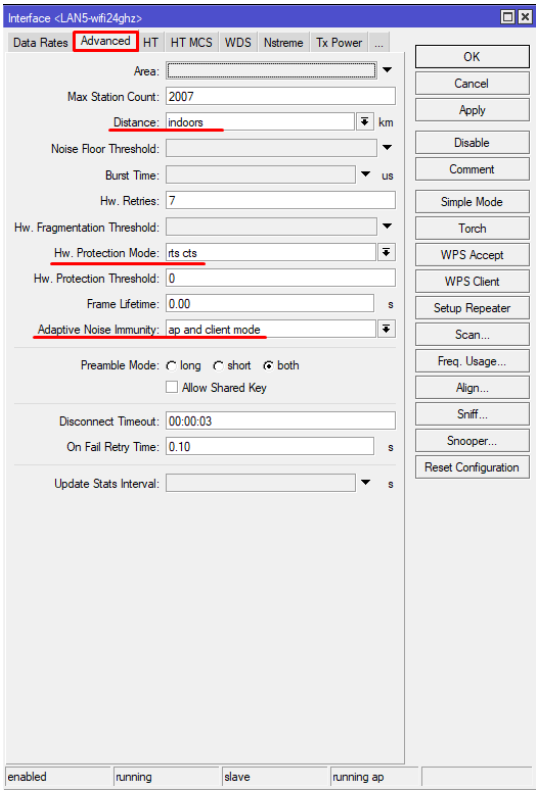

Рисунок 6.12 – Налаштування вкладки Advanced інтерфейсу WiFi 2.4GHz

Distance - Як довго чекати підтвердження одноадресних фреймів, перш ніж вважати передачу невдалою. Якщо використовуємо в невеликому приміщенні, ставимо indoors, якщо на вулиці або в цеху, то dynamic.

Adaptive Noise Immunity - Ця властивість діє тільки для карт на базі чіпсета Atheros.

Обираємо антени для роботи. Налаштовуємо так, як показано на рис. 6.13

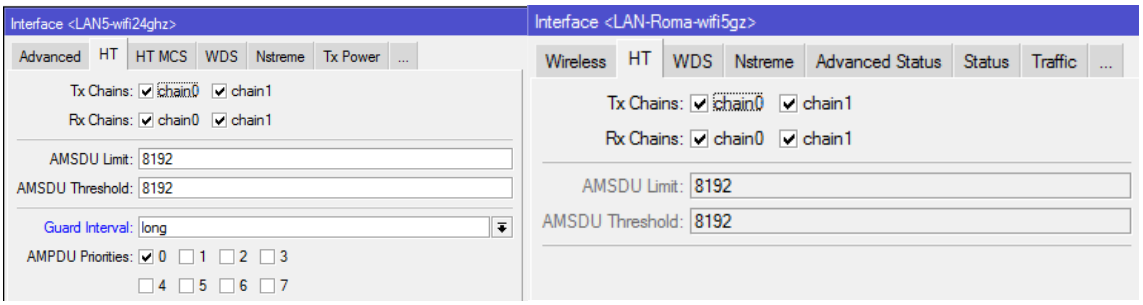

Рисунок 6.13 – Налаштування HT інтерфейсу LAN5-wifi24ghz та wifi5ghz

Опції налаштування для nstreme (рис. 6.14).

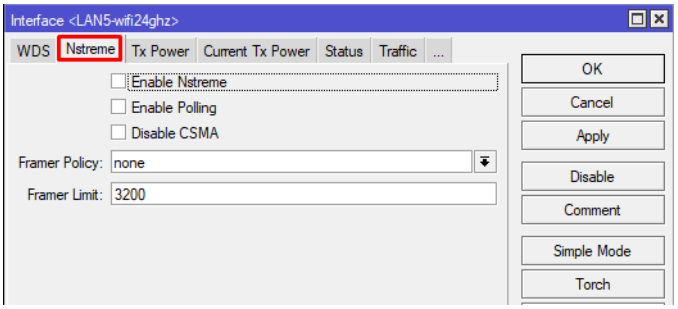

Рисунок 6.14 – Налаштування Nstreme інтерфейсу LAN5

Налаштування потужності (графічно):

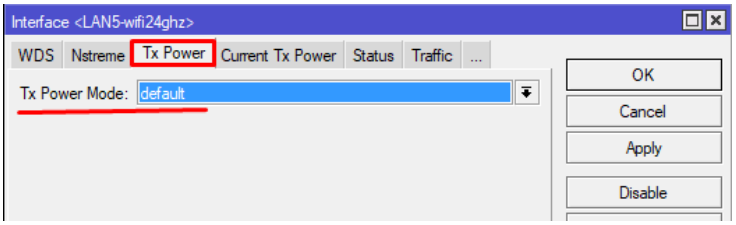

Рисунок 6.15 – Налаштування потужності сигналу

Налаштування бездротового інтерфейсу LAN5 через консоль представлено нижче:

/interface wireless set [find default-name=wlan1] adaptive-noise-immunity=ap-and-client-mode band=2ghz-onlyn channel-width=20/40mhz-Ce country=romania disabled=no distance=indoors frequency=auto frequency-mode=regulatory-domain hw-protection-mode=rts-cts mode=ap-bridge multicast-helper=full name=LAN5-wifi24ghz radio-name=POINT24_1 ssid=POINT24GHZ wireless-protocol=802.11 wmm-support=enabled wps-mode=disabled guard-interval=long

/interface wireless nstreme set LAN5-wifi24ghz enable-polling=no

На цьому налаштування інтерфейсу 2.4GHz завершені, переходимо до конфігурації інтерфейсу 5GHz.

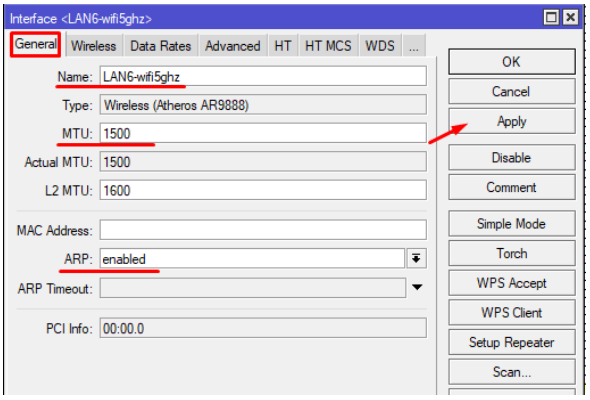

Рисунок 6.16 – Налаштування інтерфейсу 5GHz через графічний спосіб

Змінюємо ім'я інтерфейсу, MTU, і переконуємося, що ARP включено.

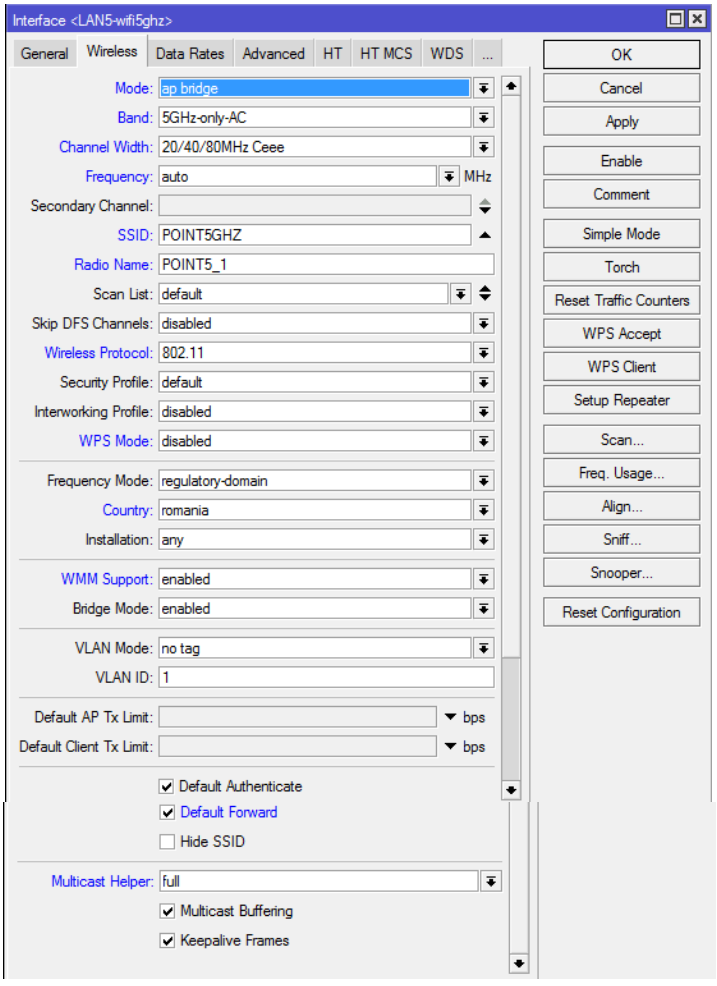

Рисунок 6.17 – Задані налаштування Wireless

Не забуваємо й про Advanced режим. Всі налаштування ідентичні тим, що встановлюються для 2.4GHz (рис. 6.18).

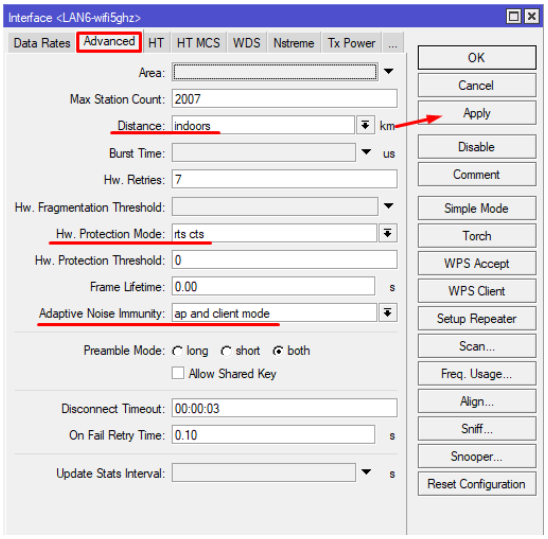

Рисунок 6.18 – Задані розширені налаштування Advanced

Теж саме, що і для 2.4GHz (рис. 6.19-21).

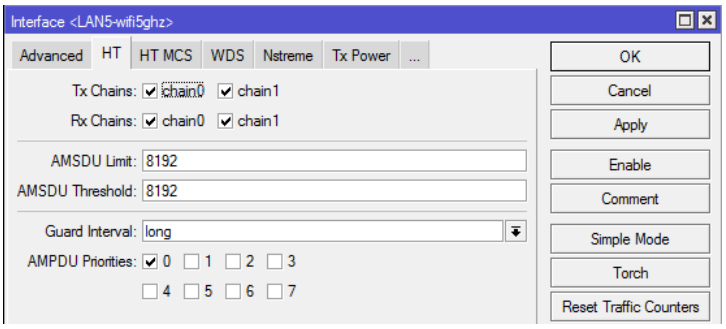

Рисунок 6.19 – Задані налаштування HT

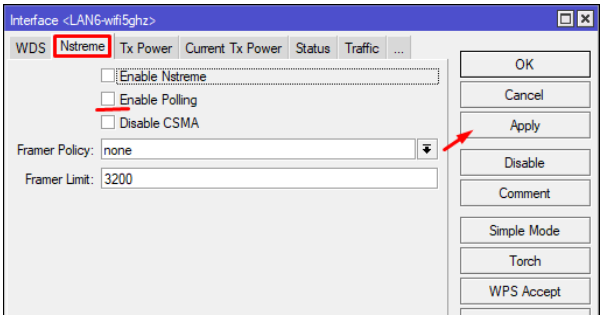

Рисунок 6.20 – Задані налаштування Nstreme

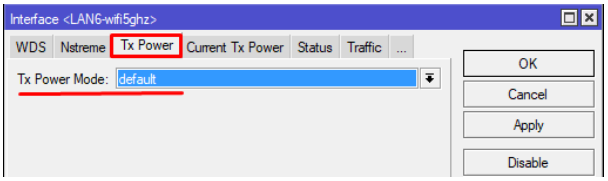

Рисунок 6.21 – Задані налаштування потужності сигналу

Приклад налаштування інтерефейсу 5GHz через консоль:

/interface wireless set [find default-name=wlan2] adaptive-noise-immunity=ap-and-client-mode band=5ghz-onlyac channel-width=20/40/80mhz-Ceee country=romania disabled=no distance=indoors frequency=auto frequency-mode=regulatory-domain hw-protection-mode=rts-cts mode=ap-bridge multicast-helper=full name=LAN6-wifi5ghz radio-name=POINT5_1 ssid=POINT5GHZ wireless-protocol=802.11 wmm-support=enabled wps-mode=disabled guard-interval=long

/interface wireless nstreme set LAN6-wifi5ghz enable-polling=no

Налаштування інтерфейсу 5GHz завершено.

Створимо мережевий міст всіх наших інтерфейсів, відповідний пункт налаштувань позначено на рис. 6.22.

Мережевий міст буде слугувати основним інтерфейсом, який об’єднає усі фізичні інтерфейси. Для цього їх необхідно додати до мережевого мосту.

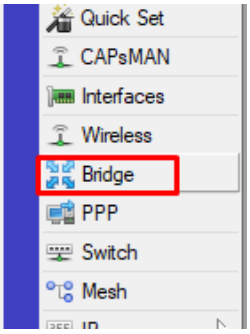

Рисунок 6.22 – Розтащування інтерфейсу Bridge у меню WinBox

Відкриваємо зазначене меню, і, для спочатку створимо сам мережевий міст із назвою **LAN-Bridge,** як показано на рис. 6.23.

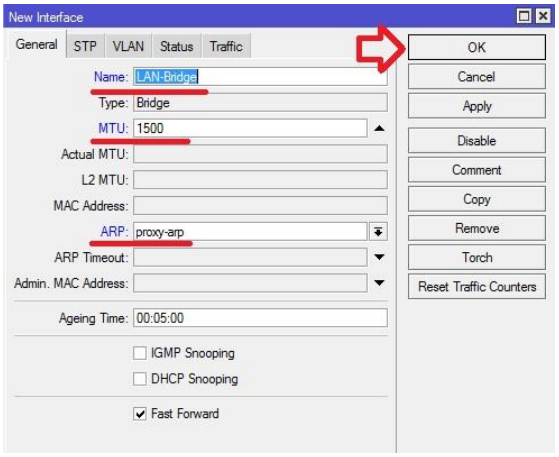

Рисунок 6.23 – Створення мережевого мосту

Приклад створення мережевого мосту через консоль:

/interface bridge add name="LAN-Bridge" comment="LAN" mtu=1500 arp=proxy-arp

Починаємо додавати порти (Рис. 6.24).

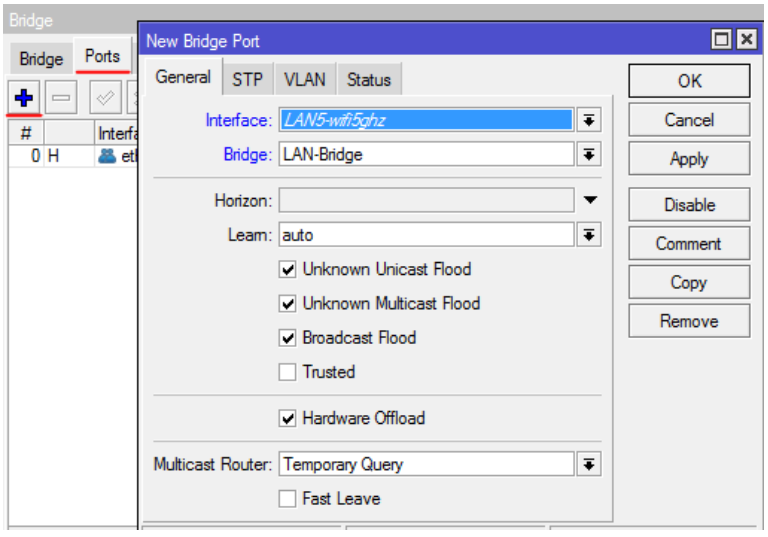

Рисунок 6.24 – Додавання портів до інтерфейсу LAN-Bridge

Для кожного потрібного порту нам потрібно додати інтерфейси:

ether2 – ether5

LAN5-wifi24ghz

LAN6-wifi5ghz

Приклад додавання портів через консольну команду:

/interface bridge port

add bridge=LAN-Bridge interface=ehter2

add bridge=LAN-Bridge interface=LAN5-wifi5ghz add bridge=LAN-Bridge

interface=LAN5-wifi24ghz add bridge=LAN-Bridge interface=ether3 add bridge=LAN-Bridge interface=ether4 add bridge=LAN-Bridge interface=ether5

У момент додавання інтерфейсу LAN1-Master Вас може відключити від маршрутизатора, в цьому немає нічого страшного, просто підключаємося знову.

4. Дозволимо нашому маршрутизатору обробляти DNS:

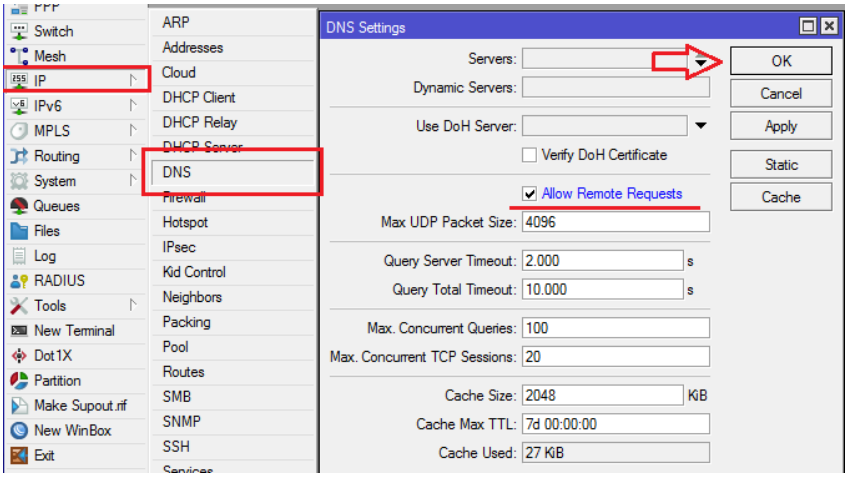

Рисунок 6.25 – Увімкнення обробки DNS на маршрутизаторі

Налаштування через консоль:

Дозволяємо обробку DNS запитів

/ip dns set allow-remote-requests=yes cache-size=4096

5. Підключення до провайдера. Необхідно налаштувати DHCP клієнт на порт в який вставлений кабель провайдера (WAN), як показано на рис. 6.26.

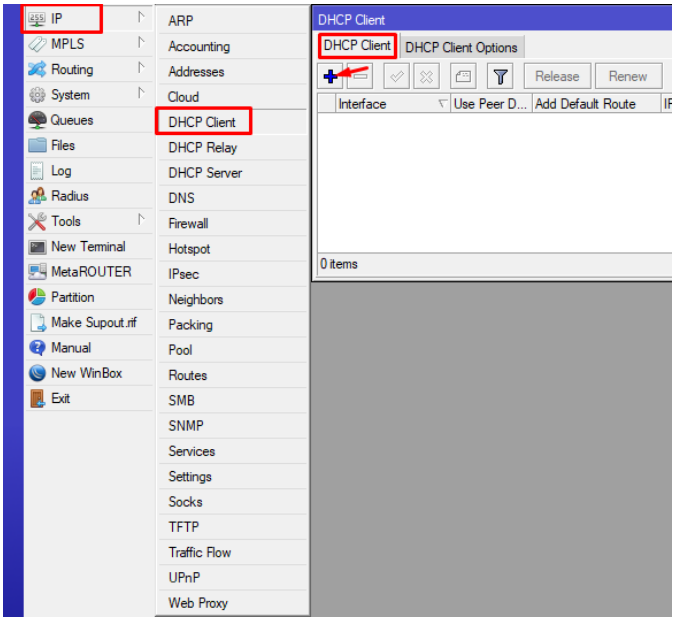

Рисунок 6.26 – Створення DHCP-клієнта

Знаходимо у потрібне меню і додаємо новий клієнт. Вказуємо потрібний інтерфейс (рис. 6.27).

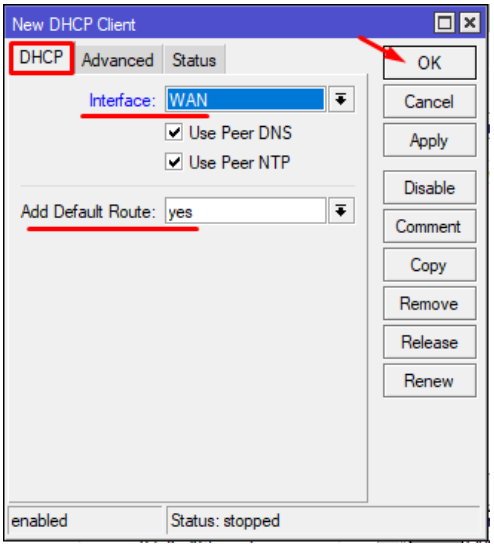

Рисунок 6.27 – Додавання нового клієнта DHCP

Налаштування через консоль буде наступним:

/ip dhcp-client add interface=WAN add-default-route=yes disabled=no default-route-distance=1 use-peer-dns=yes use-peer-ntp=yes

6. Доступ в інтернет

Для того, щоб наші користувачі могли виходити в мережу інтернет, нам необхідно вказати, через який інтерфейс вони будуть це робити. Ці налаштування робляться через Брандмауер (Firewall), як показано на рис. 6.28.

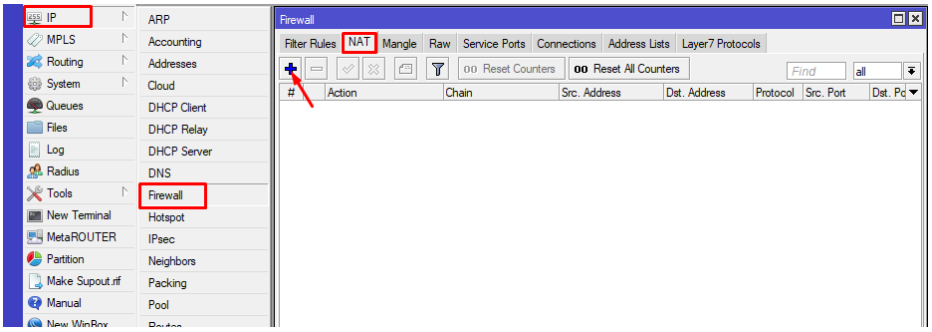

Рисунок 6.28 – Створення правила NAT

Натискаємо на «+» та прописуємо налаштування цього правила (рис. 6.29).

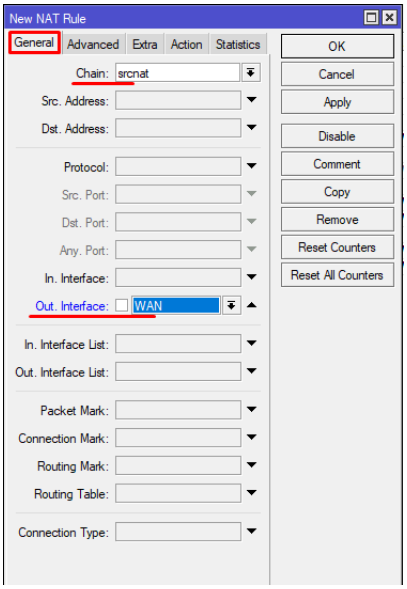

Рисунок 6.29 – Налаштування основних параметрів правила NAT

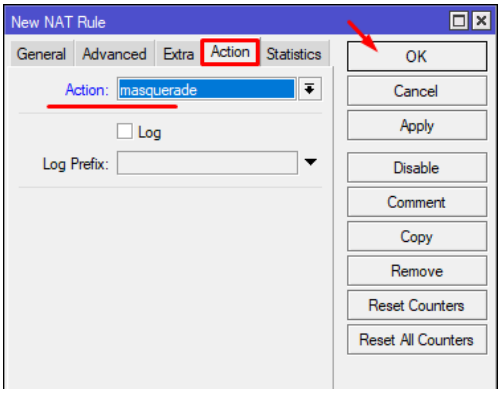

Рисунок 6.30 – Налаштування дії правила NAT

Вказуємо останнє правило і натискаємо OK. Цього достатньо, щоб на маршрутизаторі з'явився інтернет. Але у користувачів його ще не буде тому що немає IP адреси і локального DHCP сервера.

Приклад налаштування NAT через консоль:

/ip firewall nat add add action=masquerade chain=srcnat out-interface=WAN

7. IP адреса роутера. Тепер призначимо нашому маршрутизатору IP-адресу. В локації 1 буде наступна адресація: IP адреса роутера: 192.168.88.1, IP-адреси для клієнтів: 192.168.88.5 - 192.168.88.29 (Рис. 7.31-32).

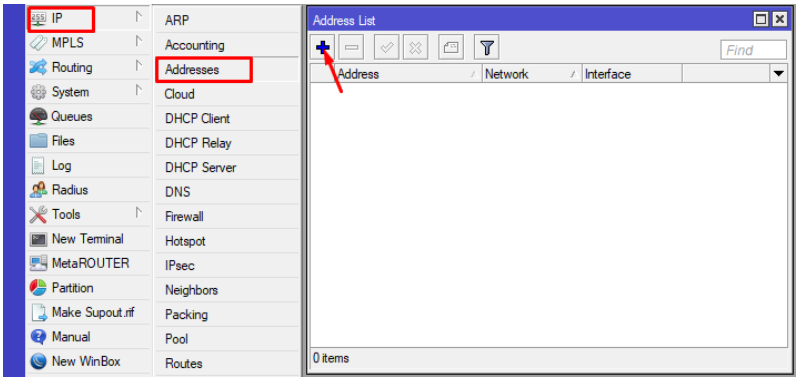

Рисунок 6.31 – Меню додавання IP-адрес

Додаємо нову IP-адресу (рис. 6.32).

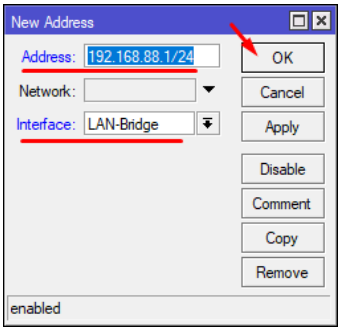

Рисунок 6.32 – Додавання нової IP-адреси

Додаємо IP-адресу для нашого мережевого моста. Цим ми вказуємо, що IP-адреса 192.168.88.1 буде прив'язана до інтерфейсу LAN-Bridge.

Приклад додавання IP-адреси через консоль:

/ip address

add address=192.168.88.1/24 interface=LAN-Bridge network=192.168.88.0

8. DHCP Сервер для локальних клієнтів. Для того, щоб наші користувачі могли підключатися до нашого роутера і отримувати від нього IP адреси та інші параметри, необхідно налаштувати DHCP сервер. Спочатку зазначимо Pool IP-адрес (рис. 6.33).

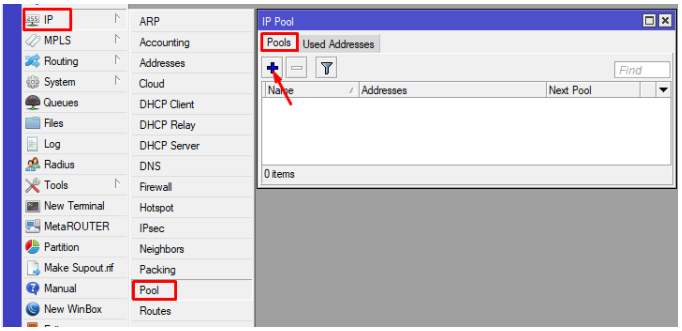

Рисунок 6.33 – Меню додавання пулу IP-адрес

Створюємо новий пул та додаємо позначений діапазон (рис. 6.34).

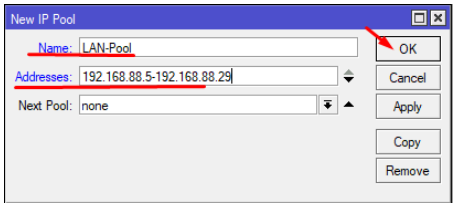

Рисунок 6.34 – Створення нового пулу DHCP

Тепер додаємо сам DHCP сервер (рис. 6.35).

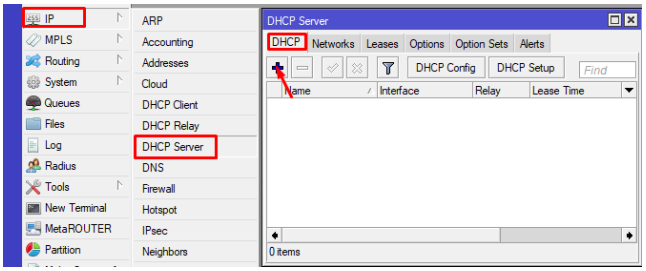

Рисунок 6.35 – Додавання DHCP сервера

Задаємо налаштування DHCP сервера (рис. 6.36).

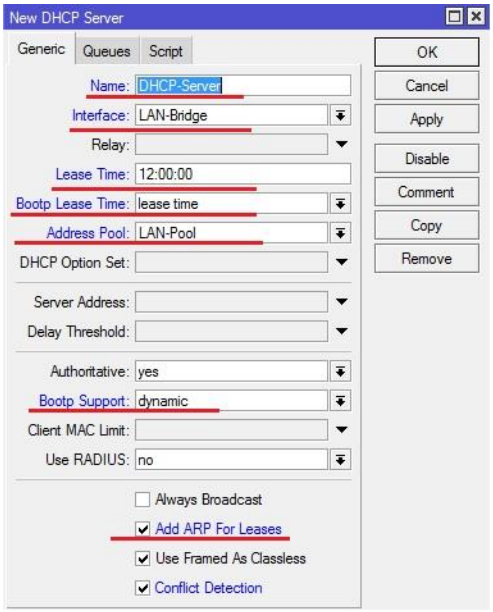

Рисунок 6.36 – Задані налаштування для DHCP сервера

Залишилося ще вказати для якої мережі і які додаткові параметри будуть отримувати підключені клієнти (рис. 6.37).

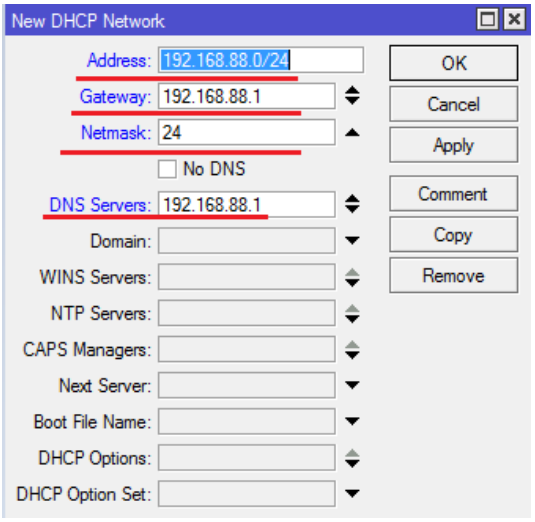

Рисунок 6.37 – Створення DHCP мережі

Вказуємо додаткові параметри. Кожен підключений клієнт буде отримувати від DHCP сервера набір параметрів: Шлюз і DNS - В нашому випадку і тим і іншим буде виступати сам роутер.

Приклад налаштування DHCP через консоль:

```
/ip pool
add name=LAN-Pool ranges=192.168.88.5-192.168.88.29
/ip dhcp-server
add add-arp=yes address-pool=LAN-Pool bootp-lease-time=lease-time \
    bootp-support=dynamic interface=LAN-Bridge lease-time=12h name=\
    DHCP-Server
```

Налаштування маршрутизатора завершено.

Завдання на лабораторну роботу

1. Провести оновлення операційних систем і пакетів на бездротовому маршрутизаторі hAP-AC^2.
2. Провести налагодження параметрів hAP-AC^2. Провести налагодження параметрів IP-адресації пристроїв мережі.
3. Превірити працездатність бездротової мережі шляхом підключення до маршрутизатора кінцевих пристроїв.

Лабораторна робота №7. Налагодження то дослідження роумінгу в безпровідній мережі побудованій за технологією CAPsMAN від Mikrotik.

Мета заняття: навчитися налаштовувати контролер керованих точок доступу на основі технології CAPsMAN та підключати бездротові точки доступу cAP; налагодити захист бездротової мережі; налаштувати та дослідити роумінг в бездротовій мережі.

Теоретичні відомості

Загальні відомості про виробника

MikroTik − латвійській виробник мережевого устаткування. Компанія розробляє та пропонує Ethernet та бездротове мережеве обладнання, зокрема маршрутизатори, мережеві комутатори, точки доступу, а також програмне забезпечення - операційні системи, RouterOS, та допоміжні продукти (рис. 6.1). Компанію було засновано у 1996 році з метою продажу обладнання на ринках, які розвиваються.

RouterOS − мережева операційна система на базі Linux, розроблена латвійською компанією MikroTik та призначена для встановлення на маршрутизаторах RouterBoard виробництва цієї ж однойменної фірми. Існує можлівість встановлення даної системи на ПК, що дозволяє наділити пристрій деякими функціями маршрутизатора ("перетворення" в брендмауер, VPN - сервер/клієнт, QoS, точку доступу тощо). Система також може служити в якості Captive - порталу на основі бездротового доступу. RouterOS підтримує безліч сервісів та протоколів, які можуть бути використані середніми або великими провайдерами - таких, як OSPF, BGP, VPLS/MPLS. RouterOS забезпечує підтримку практично всіх мережевих інтерфейсів на ядрі Linux та надає системному адміністратору графічний інтерфейс (WinBox) для наочної та швидкої конфігурації пристрою.

Загальні відомості про RouterBOARD

RouterBOARD - апаратна платформа від MikroTik, що представляє собою лінійку маршрутизаторів під управлінням операційної системи RouterOS (рис. 7.1). Різні варіанти RouterBOARD дозволяють вирішувати на їх основі різні

варіанти мережевих завдань: від простої бездротової точки доступу та керованого комутатора, до потужного маршрутизатора з брандмауером та QoS. Практично всі моделі RouterBOARD пристроїв мають підтримку живлення через PoE та роз'єм для підключення зовнішнього джерела живлення. Моделі, призначені для роботи з бездротовими технологіями, мають слот (miniPCI/miniPCIe) для підключення радіомодулів. Більшість моделей також має роз'єм для підключення до COM-порту ПК. У бюджетних моделях або в залежності від конкретного призначення моделі, ті чи інші елементи можуть бути відсутніми.

Рисунок 7.1 − Зовнішній вигляд маршрутизатора RB2011L-IN

Порядок налагодження CAPsMAN

Контролер безпровідних точок CAPsMAN (Controlled Access Point system Manager) входить в стандартний пакет інсталяції останніх версій RouterOS. Точки доступу MikroTik останніх моделей - cAP-2nD, hAP Lite тощо, повністю підтримують управління за допомогою цього програмного забезпечення, також, оновивши RouterOS, можна використовувати контролер і на більш старому обладнанні. CAPsMAN встановлюється на маршрутизатор, який буде виконувати роль центрального пристрою управління точками, причому це може бути маршрутизатор і без бездротового модуля. Для роботи коректної роботи пристрою, повинна бути встановлена RouterOS не нижче версії 6.11. CAPsMAN v.2 працює, починаючи з версії RouterOS v6.22rc7. Точки доступу підключаються до маршрутизатора з встановленим CAPsMAN за допомогою витої пари, а також можуть підключатись одне до одного послідовно (також за допомогою витої пари).

Оновлення RouterOS

Перше, що необхідно зробити перед налаштуванням CAPsMAN - оновити програмне забезпечення пристроїв.

Для цього потрібно скинути налаштування маршрутизатора до заводських:

RB2011UiAS-2HnD-IN можна скинути як за допомогою кнопки Reset, яка знаходиться на задній панелі пристрою між антенами (утримувати її до тих пір, поки зелений світлодіод не почне блимати і відпустити), так і за допомогою отвору джампера на дні роутера, розташованого під кнопкою Reset (вставити в отвір викрутку, ввімкнути пристрій, зачекати 10 секунд до скидання конфігурації).

Рисунок 7.2 – Розташування кнопки Reset на задній панелі пристрою

MikroTik cAP-2nD також необхідно скинути до заводських налаштувань за допомогою кнопки Reset, розташованої зліва від порту Ethernet (рис. 7.3). Для цього потрібно утримувати її, поки світлодіоди не почнуть блимати і потім відпустити.

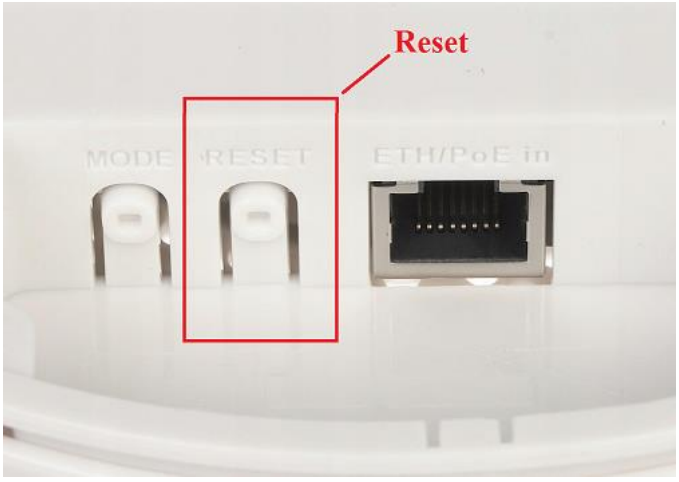

Рисунок 7.3 – Розташування кнопки Reset на нижній панелі cAP-2nD

Далі на офіційному сайті (https://mikrotik.com/download) завантажується відповідна прошивка. Для обох пристроїв підходить одна і та ж - mipsbe.

Прошивати точки за допомогою програми netinstall.

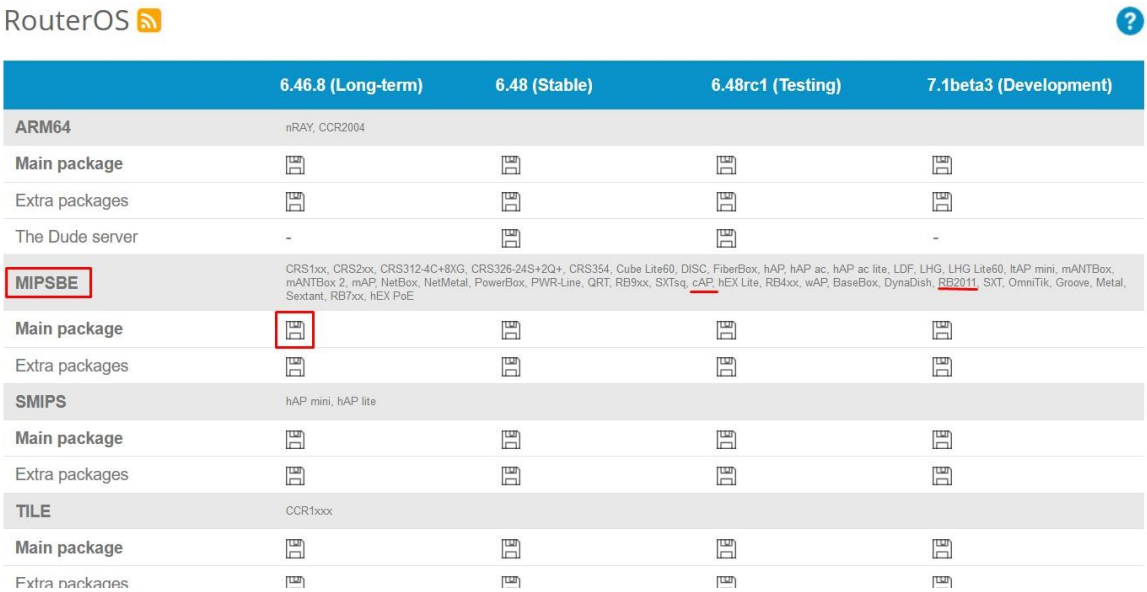

Рисунок 7.4 − Завантаження нової версії RouterOS

Підключаємо RB2011UiAS-2HnD-IN до комп'ютера для налаштування. Наприклад, підключаємо кабель в порт ETH6, але можна підключати до будь-якого порту, **крім першого**. Мережеві налаштування комп'ютера повинні бути попередньо налаштовані таким чином, щоб маршрутизатора та мережева карта комп'ютера мали адреси однієї підмережі. IP-адреса пристроїв MikroTik за замовчуванням - *192.168.88.1*, **логін** - *admin*, **пароль** - порожній.

Запускаємо WinBox, заходимо на маршрутизатор. У першому вікні скидаєтсья конфігурація за замовчуванням. Якщо вхід відбувався за IP-адресою, WinBox в цьому місці відключиться, так як налаштування скинуті і IP-адреса пристрою в тому числі. Заходимо ще раз, **натискаючи на MAC-адресу,** а потім на пункт “Connect”. Для оновлення необхідно зайти в меню **Files**. Відкриваємо його і перетягуємо в це вікно наш завантажений файл з новою прошивкою. Підтверджуємо оновлення.

Після закінчення завантаження файлу з прошивкою необхідно зайти в меню System і натиснути пункт Reboot. Роутер перезавантажиться і оновить прошивку. Зверніть увагу, що це може бути довгий процес - 3-5 хвилин. **Відключати живлення під час процесу оновлення не можна!** Перевіряємо, чи коректно оновився завантажувач. Відкриваємо в меню System - RouterBoard і перевіряємо,

чи збігаються версії в полях Current Firmware та Upgrade Firmware. Якщо ні - тиснемо кнопку Upgrade і перезавантажуємо пристрій (Рис. 7.5).

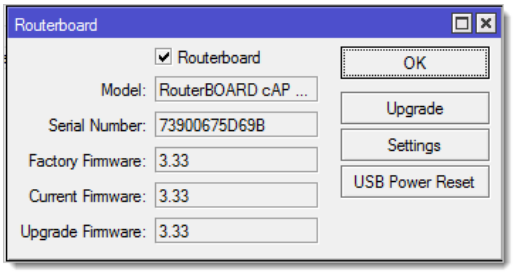

Рисунок 7.5 −Інформація про версію ОС

Налаштування маршрутизатора з контролером CAPsMAN

Проводимо налаштування RB2011UiAS-2HnD-IN у вкладці QuickSet, встановивши режим Ethernet та обравши Bridge mode, як на Рис. 7.6.1-2. Якщо режим Ethernet відсутній у списку, встановіть режим «WISP AP» (Рис. 7.6.2).

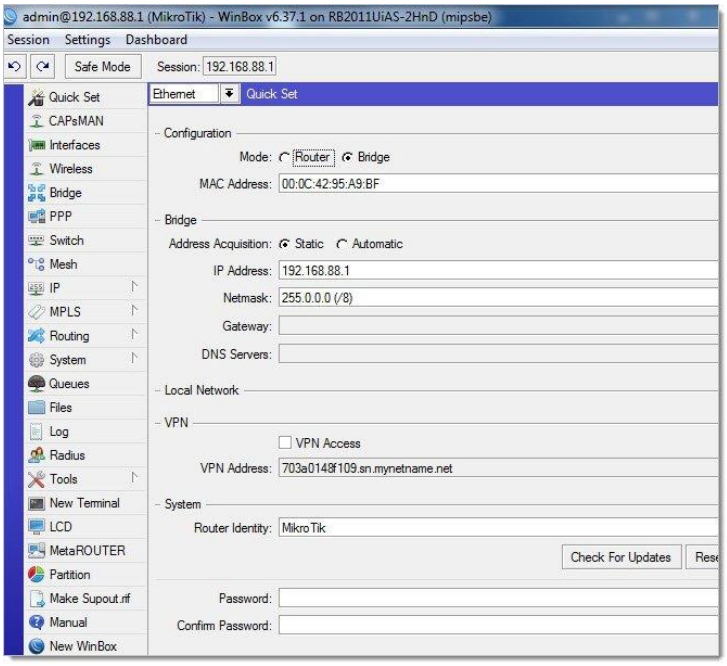

Рисунок 7.6.1 − Налаштування Quick Set з режимом Ethernet

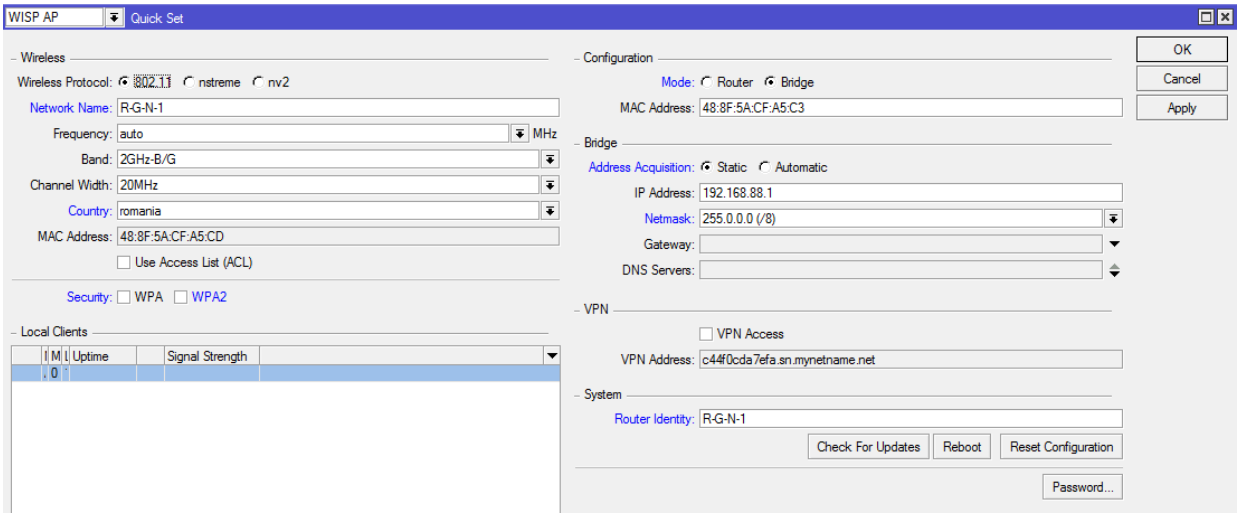

Рисунок 7.6.2 – Налаштування Quick Set з режимом WISP AP

Далі необхідно об’єднати всі порти і канали WiFi пристрою в єдиний bridge (щоб точки, підключення через WiFi та по дротовій мережі могли бачити один одного). Для цього потрібно зайти у вкладку Interface і створити новий (плюс зверху зліва), в випадаючому меню обрати bridge і дати йому нове ім'я. Налаштування бриджу в результаті виглядають так (Рис. 7.7-8):

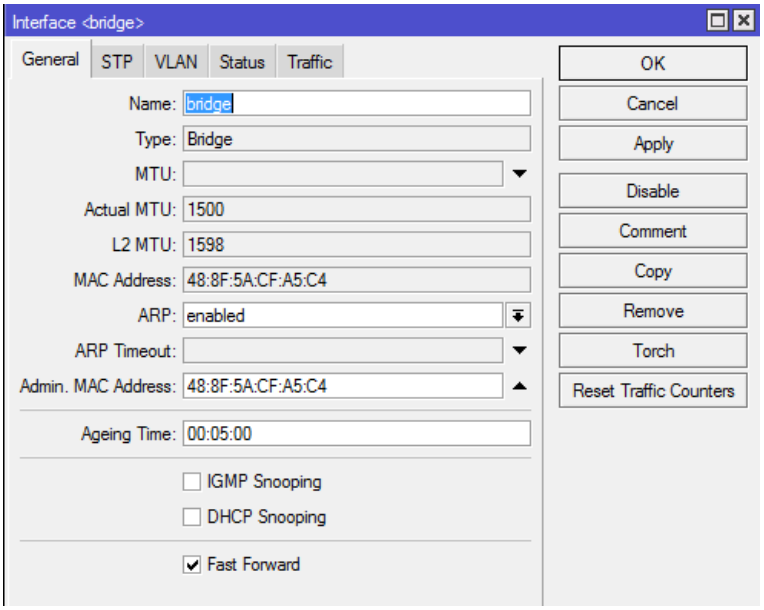

Рисунок 7.7 − Параметри налаштування інтерфейсу bridge бездротового маршрутизатора RB2011UiAS-2HnD-IN

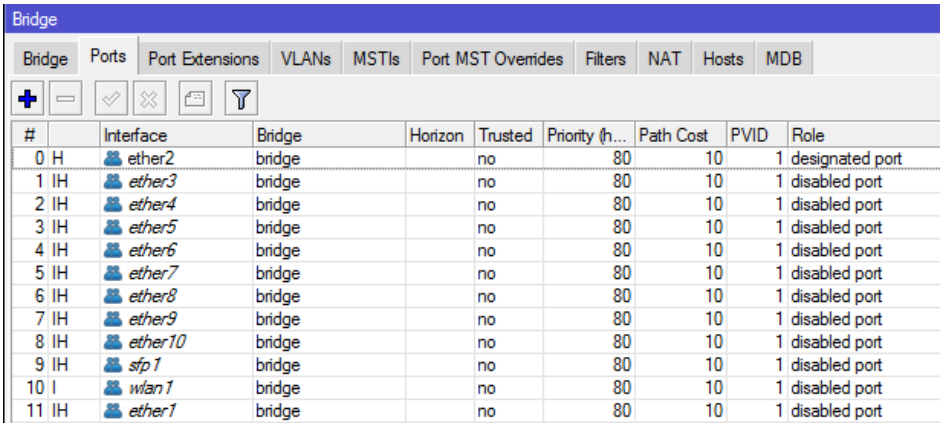

Рисунок 7.8 − Параметри налаштування портів бездротового маршрутизатора RB2011UiAS-2HnD-IN

В меню IP-Adresses потрібно прописати адресу для маршрутизатора (при налаштуванні прописано адресу за замовчуванням - 192.168.88.1). Аналогічним чином оновлюється і точки доступу MikroTik cAP-2nD, також об'єднуються їх порти в bridge1, і прописуються IP-адреси (Наприклад, для cAP-2nD адресою буде 192.168.88.28). Для випадку мережі невискокої складності (як у випадку лабораторної роботи), усі точки доступу вносяться до однієї підмережі, однак можливе налаштування CAPsMAN з пристроями в різних підмережах.

Активація модуля CAPsMAN

В останніх прошивках модуль активований за замовчуванням (він вшитий в пакет wireless), а в меню вгорі зліва завжди є вкладка CAPsMAN. В нашому випадку цей пункт можна пропустити. У випадку старої прошивки, де модуль управління CAPsMAN за замовчуванням відключений, необхідно зробити наступне. В меню System - Packages, потрібно виділити пакет wireless-cm2 і натиснути Enable. Пакет відображається як готовий до активації.

Щоб пакет активувався, потрібно перезавантажити маршрутизатор. Після перезавантаження рядок wireless-cm2 відобразиться активним, а пакет wireless-fp (застарілий) - навпаки, неактивним.

Налаштування модуля CAPsMAN

На пристрої, який буде виступати в ролі контролера точок, (в нашому випадку - на RB2011UiAS-2HnD) потрібно налаштувати керуючий модуль CAPsMAN. Для цього знаходимо вказаний пункт в меню. Заходимо в нього та вмикаємо контролер

(CAPsMAN - вкладка InterFace - Manage - відмітка в пункті Enable), як показано на Рис. 7.9.

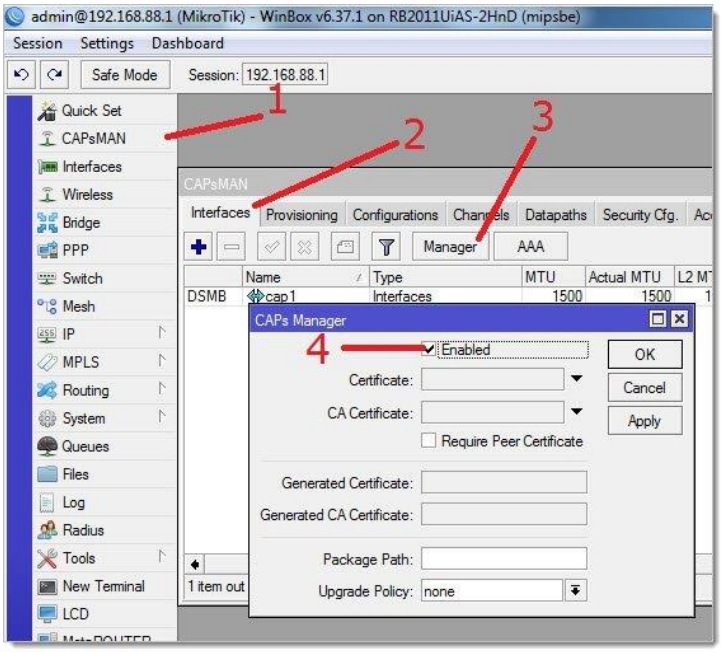

Рисунок 7.9 − Активація контролера CAPsMAN

Прописуємо потрібні налаштування Wi-Fi каналу на вкладці Channel (Рис. 7.10)

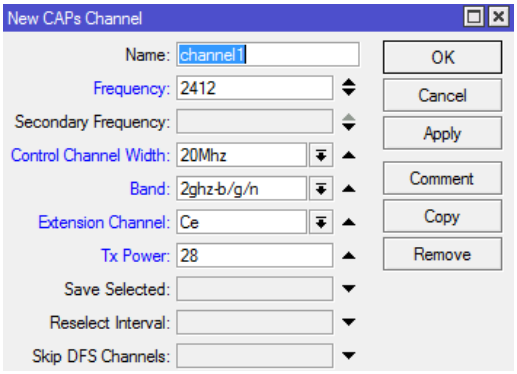

Рисунок 7.10 – Налаштування Wi-Fi каналу

Потім - налаштування Datapath, тут тільки назва, і обираємо bridge інтерфейс (ім'я залежить від того, який ви створили на попередньому етапі), як показано на Рис. 7.11.

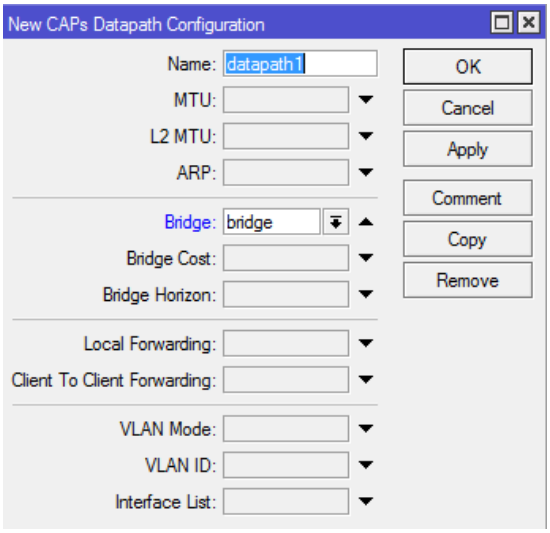

Рисунок 7.11 – Налаштування Datapath та обраний bridge-інтерфейс

Якщо встановити відмітку local-forwarding, управління трафіком передається безпосередньо до точок доступу. Якщо відмітка знята, управління трафіком бере на себе контролер (маршрутизатор).

Далі проводяться налаштування безпеки на вкладці Security (Рис. 7.12).

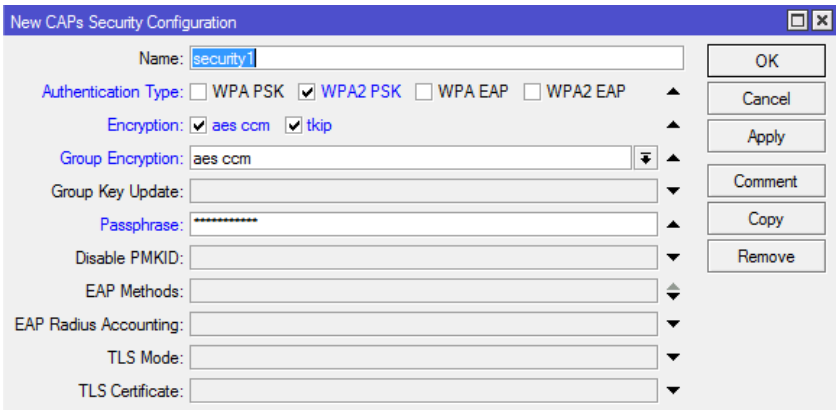

Рисунок 7.12 – Налаштування безпеки CAPsMAN

Далі на вкладці Configurations створюється нова конфігурація. У першому розділі Wireless прописується ім'я конфігурації, режим роботи, SSID мережі і активуються всі канали передачі (Рис. 7.13).

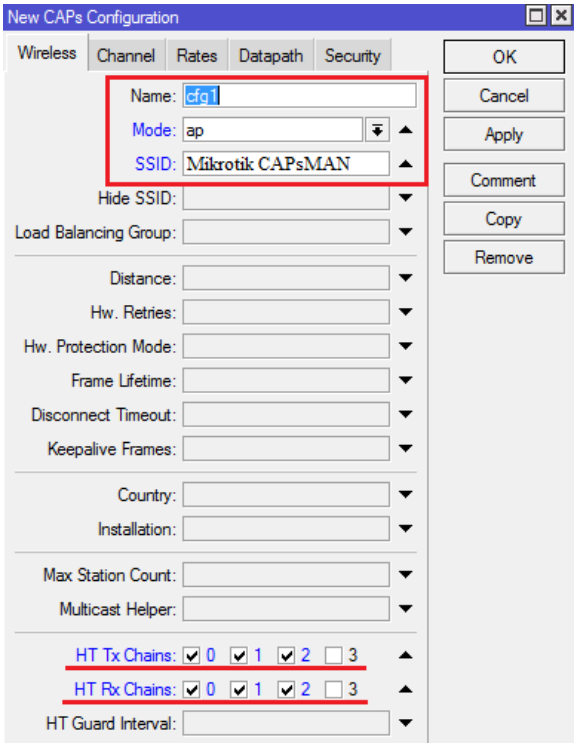

Рисунок 7.13 – Налаштований розділ Wireless у CAP’s Configuration

На інших вкладках просто обираються налаштування Channel, Datapath та Security, об'єднуючи їх в одну конфігурацію (Рис. 7.14.1).

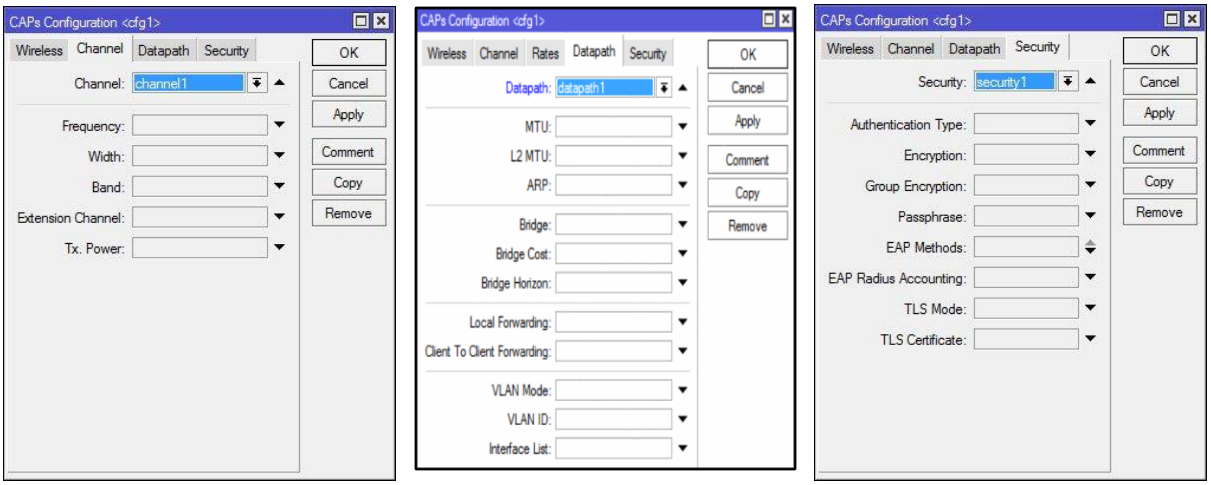

Рисунок 7.14.1 – Налаштування вкладок Channel, Datapath та Security

Далі у вкладці Provisioning або "розгортання" встановлюється правило розгортання конфігурації. Перше поле (Radio MAC) не змінюється, в полі **Action** вказують, що будуть створюватися включені за замовчуванням динамічні інтерфейси (create dynamic enabled).

Налаштування точки доступу під керуванням CAPsMAN на роутері

Бездротовий маршрутизатор RB2011UiAS-2HnD-IN крім функцій контролера

керованих безпровідних точок, сам також є точкою доступу. Тому точка доступу також налаштовується у відповідний режим, тобто прописуємо, що конфігурація має бути налаштована від контролера (CAPsMAN). Ці налаштування будуть трохи відрізнятися від налаштувань звичайних точок. В меню **Wireless**, потрібно обрати пункт **CAP**, встановити відмітку Enabled. У поле CAPsMAN Addresses прописується адреса loopback. Зі списку обирається створений раніше bridge (міст). Решта полів не змінюється (Рис. 7.15.1).

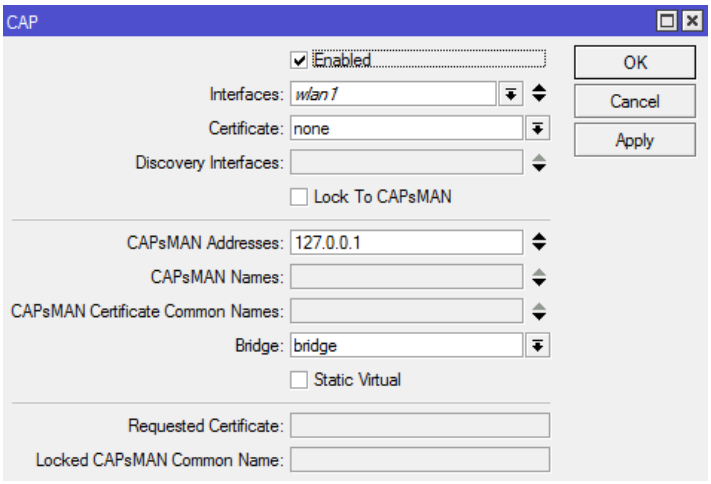

Рисунок 7.15.1 – Налаштування вбудованої точки доступу для роботи з CAPsMAN

Також небхідно створити нове правило брандамауера, інакше вбудована точка доступу не буде увімкнена! Для створення нового правила, відкрийте: IP > Firewall > Filter Rules > “+” та вкажіть параметри, показані на рис. 7.15.2. Після свторення правила, знайдіть його у кінці списку та перемістіть на місце перед правилом: “**drop all not coming from LAN**” (рис. 7.15.3).

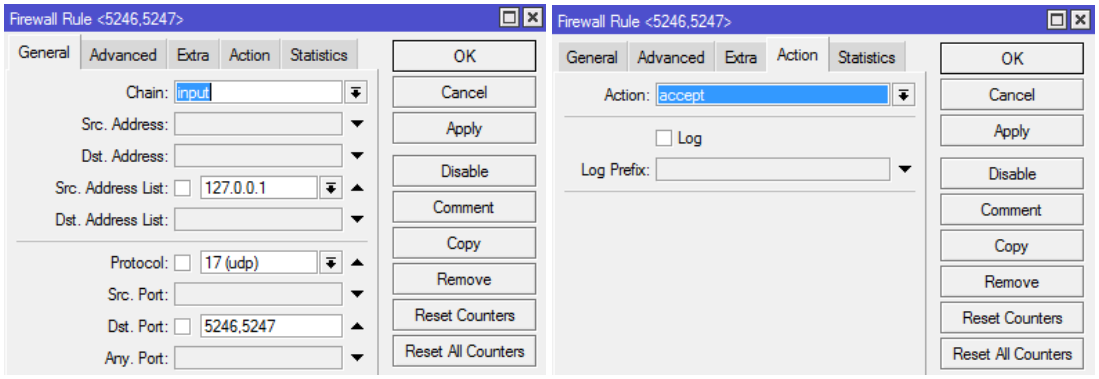

Рисунок 7.15.2 – Параметри правила

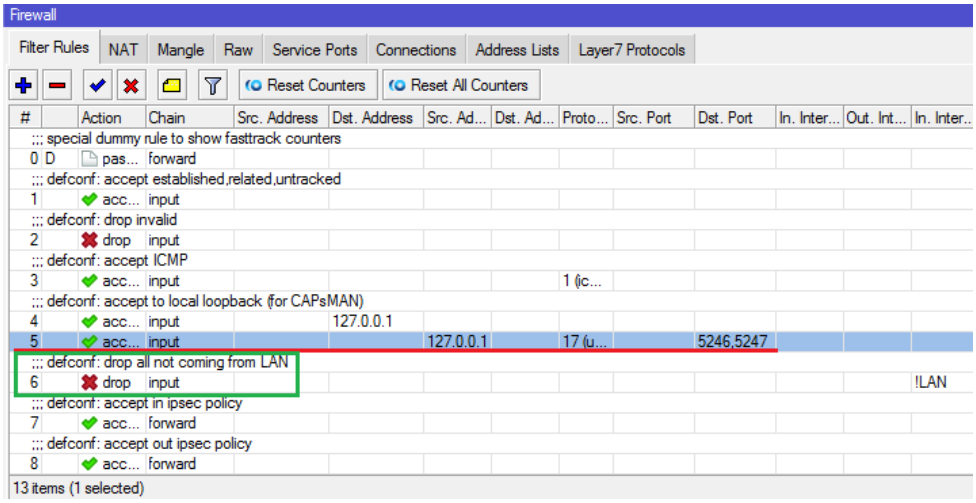

Рисунок 7.15.3 – Розміщення створеного правила у списку

Після підтвердження налаштувань, над рядком інтерфейсу повинні з'явитись червоні рядки, які повідомляють про те, що вбудована точка доступу керується CAPsMAN. Вбудована точка доступу налаштована правильно.

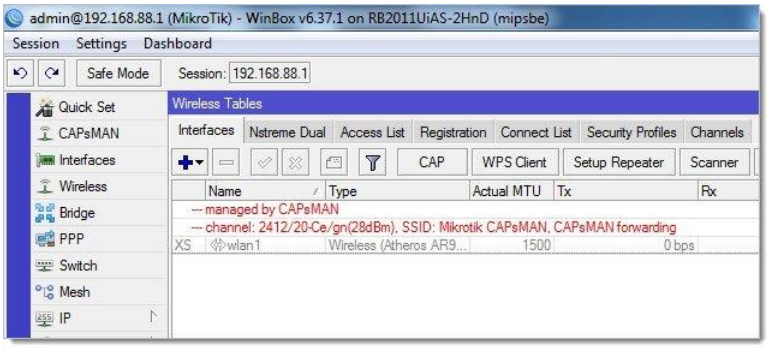

Рисунок 7.16 – Налагоджена робота точки доступу маршрутизатора від CAPsMAN

Налаштування точки MikroTik cAP-2nD під управління контролером

Налаштовуємо одну точку доступу під CAPsMAN. Перед налаштуванням необхідно виконати аналогічні дії як і для маршрутизатора: скинути до заводських параметрів, оновити прошивку до останньої версії, перевірити чи оновився завантажувач, і якщо ні, то оновити його також, об'єднати всі порти в bridge, прописати IP-адресу. На вкладці QuickSet на підключених точках доступу вказується тільки IP-адреса, інші налаштування будуть застосовані з конфігурації CAPsMAN. Далі активується (якщо необхідно) такий же пакунок, що і в роутері. У нашому випадку пакунок wireless був активний за замовчуванням (Рис. 7.17).

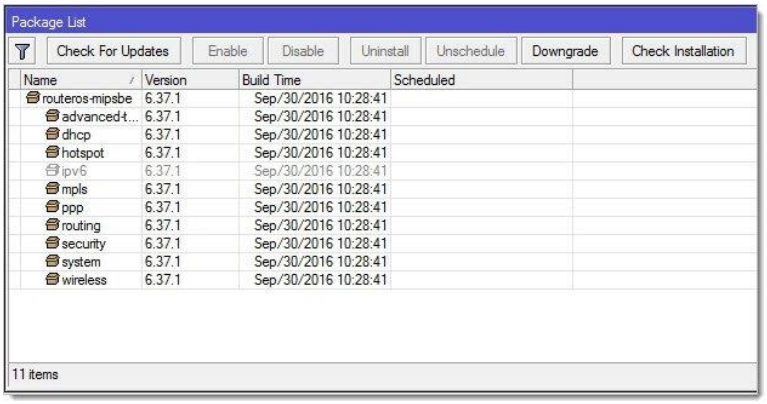

Рисунок 7.17 – Активований пакунок wireless точки доступу cAP

Важливо: на всіх пристроях CAPsMAN повинен бути однакової версії.

Далі в меню **Wireless**, обираємо пункт **CAP**, вмикаємо опцію **Enabled**. Від аналогічного налаштування на маршрутизаторі, заповнення інших полів відрізняється тим, що замість адреси CAPsMAN ми вказуємо Discovery Interfaces, тобто інтерфейси, через які cAP повинна підключатися до контролера - в нашому випадку через **bridge** (Рис. 7.18).

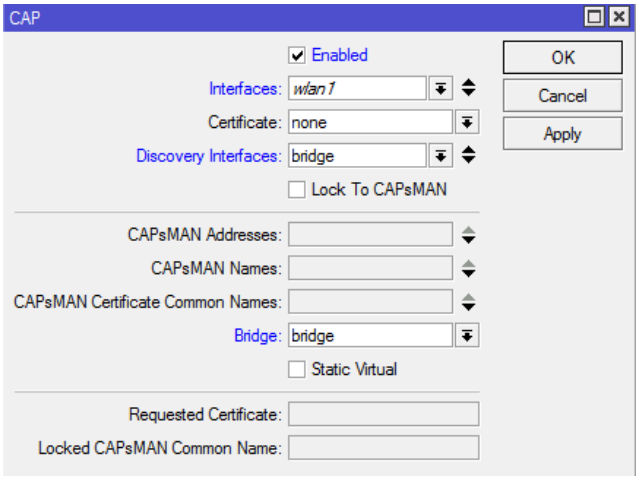

Рисунок 7.18 – Налаштування CAP для точки доступу cAP

Зберігаємо налаштування і через кілька секунд над бездротовим інтерфейсом повинні по черзі з'явитись дві нові рядки. Це говорить про те, що точка підключена до контролера CAPsMAN, завантажила вказану конфігурацію і тепер перебуває під його керуванням (Рис. 7.19).

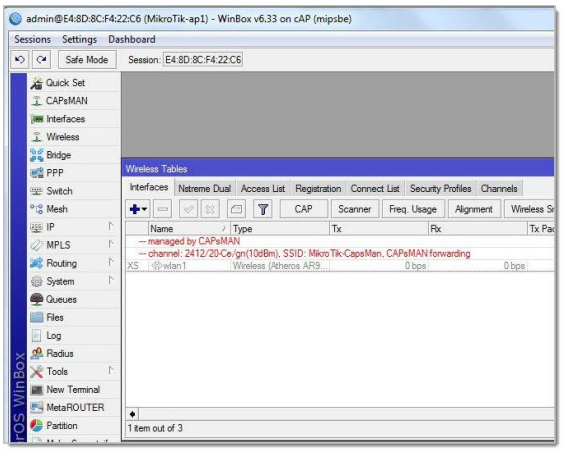

Рисунок 7.19 – Налаштована та підключена точка доступу cAP до контролера

Повернувшись до маршрутизатору, ми побачимо, що в розділі CAPsMAN з'явилися нові бездротові інтерфейси точок доступу (Рис. 7.20).

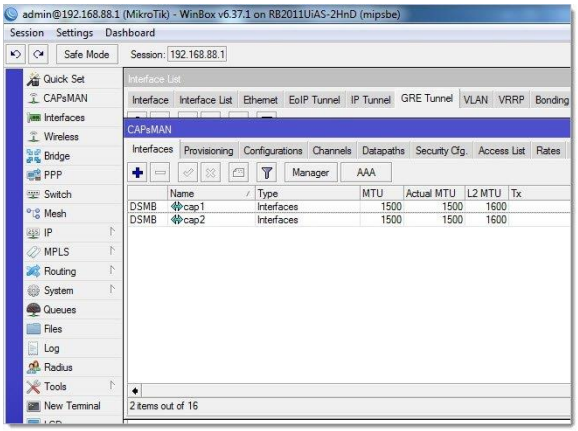

Рисунок 7.20 – Підключені точки доступу до контролера CAPsMAN

Ці ж інтерфейси можна спостерігати і в загальному розділі (Рис. 7.21).

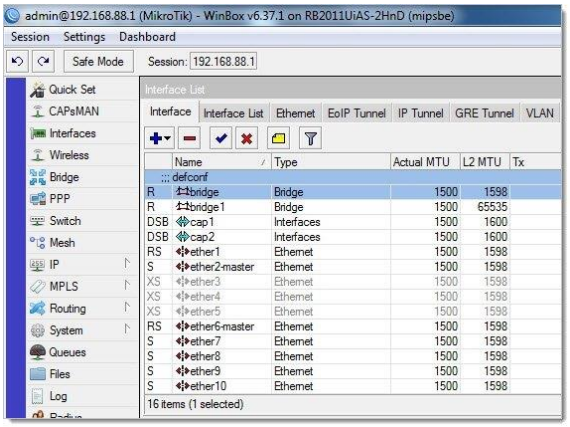

Рисунок 7.21 − Підключені точки доступу у списку інтерфейсів

Налаштування модуля CAPsMAN на цьому завершено.

Завдання на лабораторну роботу

1. Провести оновлення операційних систем та пакунків на бездротовому роутері RB2011UiAS-2HnD-IN і точках доступу cAP-2nD;
2. Використовуючи бездротовий маршрутизатор RB2011UiAS-2HnD-IN та точки доступу cAP-2nD зібрати мережу на Рис. 7.22;

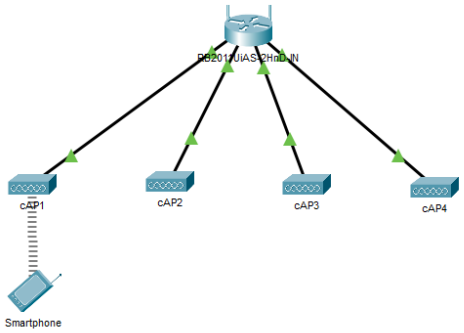

Рисунок 7.22 − Проєкт мережі

3. Розробити схему адресації пристроїв мережі;
4. Провести налагодження параметрів контролеру CAPsMAN. Провести налагодження параметрів IP-адресації пристроїв мережі;
5. Превірити працездатність отриманої безпровідної мережі шляхом підключення до точок доступу та маршрутизатора;
6. Перевірити працездатність роумінгу безпровідної мережі під керуванням контролера CAPsMAN.

Лабораторна робота № 8. Створення системи контролю доступу з оповіщенням про проникнення в середовищі Cisco Packet Tracer

Метою даної практичної роботи є отримання базових навичок по програмуванню SBC і на мові Python в середовищі Cisco Packet Tracer.

Завдання на практичну роботу

- Побудувати систему контролю доступу
- Підключити систему оповіщення про проникнення до Telegram-боту

Хід роботи:

1. Створіть проєкт системи контролю доступу, що складається з трьох датчиків руху, як показано на Рис. 8.1.

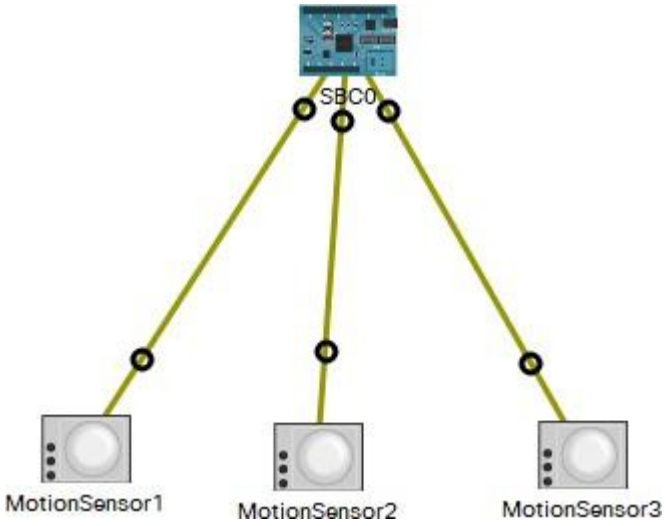

Рисунок 8.1 – Схема проєкту

Одноплатний комп’ютер (SBC) розташований у меню [Components] => [Boards]=>[SBC].

Рисунок 8.2 – Розташування SBC у меню компонентів

Всі елементи з’єднуються за допомогою кабелю IoT Custom Cabel (Рис. 8.3).

Рисунок 8.3 – Позначення кабелю IoT Custom Cabel

Датчик руху (Motion Sensor) підключають до цифрового виводу. Motion Sensor можна знайти в [Components] => [Sensor] (Рис. 8.4).

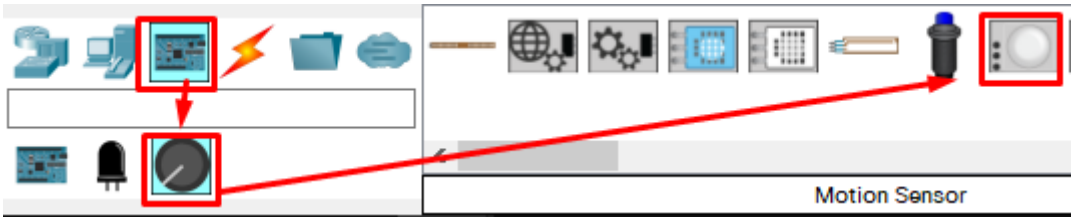

Рисунок 8.4 – Датчик руху у меню компонентів

2. Використовуючи месенджер Telegram зайдіть на сторінку для створення ботів **@BotFather** та створіть новий бот, який буде отримувати інформацію про спрацювання датчиків руху.

Рисунок 8.5 – Сторінка для створення ботів

Для цього напишіть команду /newbot. Після цього @BotFather запропонує вам вказати боту унікальні імена та посилання (name та username). На завершення ви отримаєте від @BotFather унікальний токен для вашого телеграм-бота, що дасть можливість телеграм-серверу його ідентифікувати. Приклад налаштування телеграм-бота показано на рис. 8.6.

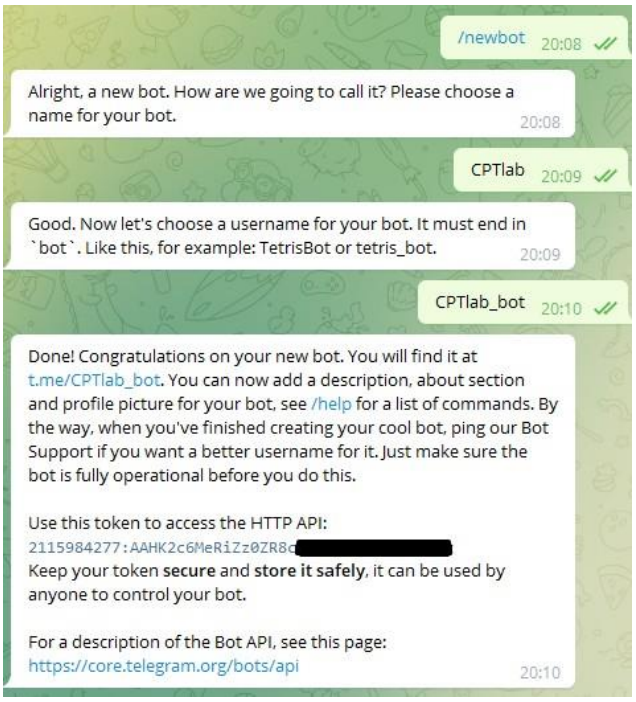

Рисунок 8.6 – Приклад створення телеграм-бота

Перейдіть за посиланням (в прикладі це t.me/CPTlab_bot) і відкрийте чат.

Далі вам потрібно отримати chat_id щоб використовувати його як місце куди надсилатимуться повідомлення від SBC. Для цього в URL браузера введіть

`https://api.telegram.org/bot<YourBOTToken>/getUpdates`

де `<YourBOTToken>` - замініть на токен вашого бота.

Наприклад:

`https://api.telegram.org/bot123456789:jbd78sadvbdy63d37gda37bd8/getUpdates` У відповідь ви отримаєте JSON об’єкт в якому і потрібно знайти chat_id

```
"chat":
    "id":           1733895254
```

Якщо GET-запит повертає порожній JSON просто з кодом 200, тоді перейдіть в чат з вашим ботом та надішліть боту команду /stop. Після цього знову надішліть GET-запит.

3. Написання програми для SBC.

Відкрийте вкладку Programming на SBC та створіть файл main.py. В створений файл *main.py* запишіть наступний код:

```
from gpio import *
from time import *
from realhttp import *
import requests


def main():
    pinMode(0,  INPUT)
    pinMode(1,  INPUT)
    pinMode(2, INPUT)

    print("System ON!")

    API_URL = "https://api.telegram.org/"
    BOT_TOKEN = "2115898477:AAHK2c6MкRiZz0ZRTc6tdj3GkBекaFP5n4k"
    SEND_METHOD = "/sendMessage"
    CHAT_ID = "chat_id=1733836254"
    TEXT = "text= "
    url = API_URL + "bot" + BOT_TOKEN + SEND_METHOD + "?" + CHAT_ID + "&" + TEXT

    def telegram_bot_sendtext():
        response = requests.get(url)

    http = RealHTTPClient()

    while True:

        sensors = {"Motion sensor 0": digitalRead(0),
                   "Motion sensor 1": digitalRead(1),
                   "Motion sensor 2": digitalRead(2)}

        for i in sensors:
            if sensors[i] == 1023:
                text = i + " is activated!"
                print(text)
                TEXT = "text=" + text
                url = API_URL + "bot" + BOT_TOKEN + SEND_METHOD + "?" + CHAT_ID
+ "&" + TEXT

                http.get(url)
                telegram_bot_sendtext()

        delay(5000)


if __name__ == "__main__":
    main()
```

В змінну BOT_TOKEN запишіть свій токен для телеграм-боту, а в CHAT_ID отриманий ідентифікатор.

Нажаль, в Cisco Packet Traser 8.x.x модуль realhttp працює з критичною помилкою, тому код містить додаткову частину, що дозволяє її обійти. Функція telegram_bot_sendtext() використовує модуль requests для формування додаткового GET-запиту, що дозволяє обійти баг з невідправкою повідомлення в чат (якщо залишити тільки http.get(url) і закоментувати наступну стрічку, то втрачатиметься повідомлення від останнього датчика). Додатковий запит від telegram_bot_sendtext() також формується помилково (не відсилається але без нього http.get(url) спрацьовує з помилкою).

Датчики руху та сигналізації в Cisco Packet Tracer працюють в форматі значень від 0 до 1023. Тому значення 1023 відповідає за наявність руху в приміщенні.

Затримка в 5 с. гарантує, що після спрацювання кожного датчика ви отримаєте тільки одне відповідне повідомлення.

4. Виконайте код кнопкою “Run”. Для активації датчика затисніть клавішу “Alt” і проведіть курсором перед датчиком активуючи його. Cisco Packet Tracer відповідним повідомленням запросить дозвіл на пересилання вашого GET-запиту до api.telegram для кожного датчика (Рис. 8.7). Дайте дозвіл для кожного повідомлення (краще для кожного окремо, для того щоб була можливість відслідковувати кількість спрацювань та можливих нових помилок в роботі коду).

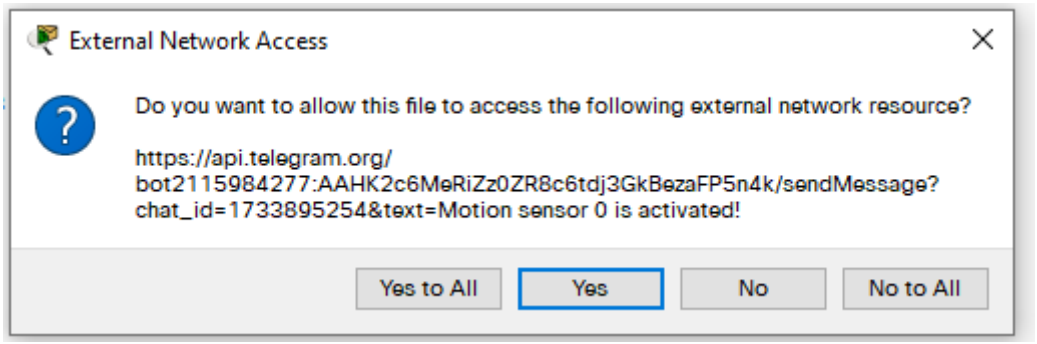

Рисунок 8.7 – Вікно із запитом на дозвіл пересилання GET-запитів

Після цього ви отримаєте в чаті вашого боту сповіщення про спрацювання відповідних датчиків, як показано на рис. 8.8.

Рисунок 8.8 – Результат роботи системи сповіщення через телеграм-бот

5. Додайте до схеми датчик пожежної сигналізації та модифікуйте відповідний код в файлі main.py. За потреби додайте ще датчики та інші IoT-пристрої для розширення функціоналу схеми. Перевірте працездатність системи та отримання відповідного сповіщення через телеграм-бот.

Запишіть висновки про виконану роботу.

Список рекомендованої літератури

1. Задерейко О. В., Багнюк Н. В., Толокнов А. А. Комп’ютерні мережі : навчально-методичний посібник [Електронне видання]. Одеса : Фенікс, 2023. URL: https://doi.org/10.32837/11300.25951 (дата звернення: 17.10.2024).
2. Ковтун О. І., Плескач В. Л., Ткаліч О. П. Бездротові мережі з використанням стандартів zig bee, bluetooth, wi-fi. *Radioelectronic and computer systems*. 2016. № 4. С. 42–47. URL: https://doi.org/10.32620/reks.2016.4.05 (дата звернення: 17.10.2024).
3. Новітні протоколи бездротових мереж: переваги та недоліки / С. Левченко та ін. *Herald of Khmelnytskyi National University. Technical sciences*. 2024. Т. 335, № 3(1). С. 445–449. URL: https://doi.org/10.31891/2307-5732-2024-335-3-61 (дата звернення: 17.10.2024).
4. Платтнер Б., Чернега В. Безпровідні локальні комп'ютерні мережі: навч. посібник. К.: Кондор, 2018. – 238 с.
5. Сайко В.Г., Казіміренко В.Я., Літвінов Ю.М. Мережі бездротового широкосмугового доступу. Навчальний посібник. – К.: ДУТ, 2015. – 196 с.
6. Одом Ю. Офіційний посібник Cisco з підготовки до CCENT/CCNA ICNDl 100-101 Acad. Ед.: транс. з англійською мовою / W. Odom. – М.: ТОВ «І. Д. Вільямс», 2015. – 912 с.
7. Cisco Meraki Fundamentals / A. Paul та ін. Pearson Education, Limited, 2024. – 368 с.
8. Coleman D. D. Wi-Fi 6 for dummies, extreme networks special edition (custom). Wiley & Sons, Incorporated, John, 2022. – 100 с.
9. Haddad M. MikroTik switching with LABS: master switching on mikrotik - all topics in the MTCSWE certification exam are covered. Independently Published, 2021.
10. Péter János V., Illési Z. Wi-Fi 6 application in iot environment. *Interdisciplinary description of complex systems*. 2022. Т. 20, № 3. С. 277–283. URL: https://doi.org/10.7906/indecs.20.3.7 (дата звернення: 17.10.2024).
11. Westcott D. A., Coleman D. D. CWNA Certified Wireless Network Administrator Study Guide: Exam CWNA-107. Wiley & Sons, Incorporated, John, 2018. − 1024 с.
12. William S. Wireless Communication Networks and Systems. Pearson Education, Limited, 2015. – С. 1−61.

ДЛЯ НОТАТОК