

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

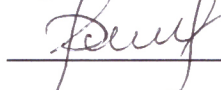
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту локальної мережі
організації, побудованої на базі технологій Ethernet та
Wi-Fi»

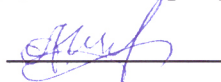
Виконав: студент 4-го курсу групи КБ-20-1
спеціальності 125 «Кібербезпека»

 Володимир КОРЖОВСЬКИЙ

Керівник: Старший викладач кафедри КІ та КБ

 Єлизавета ТРОКОЗ

Рецензент: Доцент кафедри КІ та КБ, к.т.н.

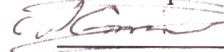
 Олексій ШЕЛУХА

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Коржовський Володимир Васильович

Тема роботи: «Проект підсистеми захисту локальної мережі організації,
побудованої на базі технологій Ethernet та Wi-Fi»

затверджена Наказом університету від 5 березня 2024 р. № 98

Термін здачі студентом закінченої роботи 9 червня 2024 р.

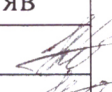
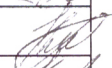
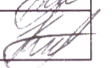
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

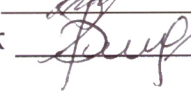
Топологія мережі; Захист локальної комп'ютерної мережі; Налаштована
технологія Wi-Fi

Обладнання та програмне забезпечення:

1. Маршрутизатор Cisco 2911
2. Комутатори Cisco Catalyst 2960
3. Бездротовий контролер Cisco® серії 2500
4. Мережевий емулятор Cisco Packet Tracer

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Трокоз Є.М.	06.03.2024 	06.03.2024 
2	Трокоз Є.М.	02.04.2024 	02.04.2024 
3	Трокоз Є.М.	03.05.2024 	03.05.2024 

Студент  Володимир КОРЖОВСЬКИЙ
Керівник  Єлизавета ТРОКОЗ

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи	Строк виконання етапів проекту	Примітки
1	Аналіз отриманого завдання та уточнення поставлених завдань	3.05.2024	виконано
2	Аналіз літературних джерел	5.05.2024	виконано
3	Аналіз об'єкта дослідження	7.05.2024	виконано
4	Постановка задачі дослідження	10.05.2024	виконано
5	Розробка структурної моделі	14.05.2024	виконано
6	Розрахунок параметрів адресації	17.05.2024	виконано
7	Вибір технології для реалізації	19.05.2024	виконано
8	Розробка КМ	22.05.2024	виконано
9	Налаштування мережі	28.05.2024	виконано
10	Адміністрування мережі	01.06.2024	виконано
11	Перевірка працездатності	03.06.2024	виконано
12	Оформлення пояснювальної записки	04.06.2024	виконано
13	Оформлення презентації	07.06.2024	виконано
14	Захист кваліфікаційної роботи		

Студент  Володимир КОРЖОВСЬКИЙ
Керівник  Єлизавета ТРОКОЗ

АНОТАЦІЯ

Пояснювальна записка до випускної кваліфікаційної роботи на тему «Проект підсистеми захисту локальної мережі організації, побудованої на базі технологій Ethernet та Wi-Fi» складається з вступу, трьох розділів, висновків, списку використаної літератури та додатку.

Текстова частина викладена на 69 сторінках друкованого тексту. Пояснювальна записка має 69 сторінок та додатки на 10 сторінку. Список використаних джерел містить 17 найменувань і займає 2 сторінку. В роботі наведено 41 рисунків та 5 таблиць. Загальний обсяг роботи 79 сторінок.

У першому розділі визначено теоретичні аспекти функціонування технологій та протоколів побудови захищених локальних мереж. А саме таких технологій: DHCP, SSH і WPA2-TKIP.

У другому розділі проведено проектування захищеної локальної мережі.

У третьому розділі проведено вибір обладнання, здійснено побудову, налагодження та тестування проєктованої локальної мережі.

Висновок містить результати виконаної роботи при створенні проєкту захищеної корпоративної мережі з використанням технологій SSH і WPA2-TKIP.

У додатках представлені схема побудованої мережі та конфігураційні файли комутаторів та маршрутизаторів мереж.

КЛЮЧОВІ СЛОВА: CISCO, МЕРЕЖА, ОРГАНІЗАЦІЯ, ЗАХИСТ, DHCP, SSH і WPA2-TKIP.

ККІКБ<.КР.Б – 125 – 07 – ПЗ

Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту локальної мережі організації, побудованої на базі технологій Ethernet та Wi-Fi	Лім.	Арк.	Аркушів
Розроб.		Коржовський В.В.		25.06				
Керівник		Трокоз Є.М.		25.06			4	79
Реценз.		Шелуха О.О.		25.06		ФІКТ Гр. КБ-20-1		
Н. контр.		Трокоз Є.М.		25.06				
Зав. каф.		Сфіменко А.А.		25.06				

ANNOTATION

The explanatory note to the course project on the topic "The project of the organization's local network protection subsystem built on the basis of Ethernet and Wi-Fi technologies" consists of an introduction, three sections, conclusions, a list of used literature and an appendix.

The text part is laid out on 69 pages of printed text. The explanatory note has 69 pages and a 10-page appendix. The list of used sources contains 17 names and occupies 2 pages. The work contains 41 figures and 5 tables. The total volume of work is 79 pages.

The first chapter defines the theoretical aspects of the functioning of technologies and protocols for the construction of secure local networks. Namely the following technologies: DHCP, SSH and WPA2-TKIP.

In the second section, the design of a protected local network is carried out.

In the third section, the selection of equipment was carried out, construction, debugging and testing of the projected local network was carried out.

The conclusion contains the results of the work done in creating a project of a secure corporate network using SSH and WPA2-TKIP.

The appendices present a diagram of the constructed network and configuration files of network switches and routers.

KEYWORDS: CISCO, NETWORK, ORGANIZATION, SECURITY, DHCP, SSH and WPA2-TKIP.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ВСТУП.....	7
РОЗДІЛ 1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ЛОКАЛЬНОЇ І БЕЗПРОВІДНИХ МЕРЕЖ, ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ТА ВИМОГИ ДО НЕЇ	8
1.1 Особливості побудови сучасних локальних комп'ютерних мереж.....	8
1.2 Технології побудови локальних комп'ютерних мереж.....	10
1.3 Мережева технологія Ethernet.....	11
1.4 Огляд та порівняння бездротових технологій.....	15
1.5 Технологія бездротової передачі даних Wi-Fi	17
1.6 Основні принципи побудови і функціонування мереж IEEE 802.11	21
1.7 Особливості забезпечення захисту локальної мережі.....	29
1.8 Особливості забезпечення захисту безпроводних мереж.....	34
РОЗДІЛ 2. ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ ЛОКАЛЬНОЇ МЕРЕЖІ.....	38
2.1. Проєктування фізичної топології мережі	38
2.2. Проєктування логічної (L3) топології мережі та розробка системи IP-адресації	40
2.3. Проєктування служб та сервісів прикладного рівня	41
2.4. Проєктування підсистеми мережного захисту.....	42
2.5 Огляд основних загроз для комп'ютерної мережі.....	43
РОЗДІЛ 3. ВИБІР ОБЛАДНАННЯ, ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ ПРОЄКТОВАНОЇ ЛОКАЛЬНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ.....	45
3.1. Вибір обладнання та ОС пристроїв для розробленого проєкту мережі.....	45
3.2. Побудова та налагодження спроєктованої локальної мережі	49
3.3. Тестування роботи створеної локальної мережі.....	60
ВИСНОВКИ.....	66
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	67
ДОДАТКИ.....	69

ВСТУП

Актуальність даної теми полягає у повсякденній необхідності створення нових мереж, оптимізації та адмініструванні вже наявних, та в першу чергу розвитку мережевих технологій, їх постійне вдосконалення, зокрема винайдення нових середовищ передачі даних. Технічне завдання кваліфікаційної роботи наочно демонструє реальну задачу у реальному житті, а отже уміння, отримані за час реалізації проєкту, будуть не зайвими при виконанні аналогічної задачі з фізичним обладнанням.

Для проєктування власної мережі варто врахувати велику кількість нюансів, як приклад: визначення масштабу мережі, вибір оптимальних технологій для налагодження, встановлення засобів захисту та віддаленого доступу.

Об'єктом дослідження є процеси проєктування, налаштування та тестування захищених локальних мереж із використанням технологій Ethernet та Wi-Fi.

Предметом дослідження є методи, засоби та технології налагодження та тестування захищеної локальної мережі організації, побудованої на базі технологій Ethernet та Wi-Fi.

Метою даного дослідження є моделювання та розробка захищеної локальної комп'ютерної мережі з використанням технології SSH і WPA2-TKIP.

Завдання даного дослідження:

- проєктування та розробка захищеної локальної комп'ютерної мережі організації;
- використання технології SSH і WPA2-TKIP;
- проєктування та розробка підсистем мережного захисту;
- реалізація функціонування комп'ютерної мережі.

Практичне значення даної кваліфікаційної роботи полягає у можливості практичного використання розробленої захищеної локальної мережі у повсякденному житті.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

РОЗДІЛ 1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ЛОКАЛЬНОЇ І БЕЗПРОВІДНИХ МЕРЕЖ, ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ТА ВИМОГИ ДО НЕЇ

1.1 Особливості побудови сучасних локальних комп'ютерних мереж

Локальна мережа передавання даних (LAN) використовується для з'єднання між собою комп'ютерів, розташованих на невеликій території, за допомогою спеціальних апаратно-програмних засобів. Метою створення LAN є доступ до розміщених на інших комп'ютерах мережі розподілених ресурсів: інформаційних, програмних та технічних. До основних компонентів локальних мереж відносять:

- комп'ютери;
- програмне забезпечення мережі (мережеві операційні системи і мережеві додатки);
- комунікаційне обладнання;
- структуровані кабельні системи.

В локальних мережах можуть використовуватися комп'ютери двох типів:

1. Робочі станції, які через мережу отримують доступ до розподілених ресурсів та призначені для розв'язування прикладних задач користувача.
2. Центральний комп'ютер (сервер), який містить розподілені ресурси, доступні для інших комп'ютерів (клієнтів). Залежно від того, який тип комп'ютерів містить мережа, розрізняють два типи локальних мереж:

- однорангові мережі (мережа типу “клієнт – клієнт”);
- мережі з центральним комп'ютером (мережа типу “клієнт – сервер”).

Мережеві операційні системи складають програмну платформу комп'ютерних мереж і значною мірою визначають ефективність їх роботи цілому. До системних програмних компонентів мережі відносяться:

- протокольні модулі, які визначають і регулюють спосіб взаємодії між вузлами і модулями мережі;

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

- комунікаційні програми, які забезпечують передачу даних між компонентами мережі;
- програми апаратного рівня, які керують роботою технічних засобів мережі.

Програмні мережеві додатки зорієнтовані на задачі користувачів і забезпечують реалізацію мережевих служб. Мережевий додаток реалізується двома розподіленими програмами: програмою-клієнтом і програмою-сервером. Програма-клієнт функціонує на комп'ютері-клієнті і формує запит на обслуговування, а програма-сервер функціонує на комп'ютері, який виконує запит.

Комунікаційні пристрої локальних мереж відповідають стандартам конкретних базових технологій і підтримують передавання даних по конкретному фізичному середовищі. Вони призначені для здійснення комутації між вузлами мережі, відновлення якості електричних сигналів, збільшення мережі, фізичної та логічної структуризації локальних мереж. Фізичну структуризацію здійснюють з метою збільшення її довжини та числа комп'ютерів за допомогою повторювачів і концентраторів. Фізична структуризація дозволяє не тільки збільшити число РС і довжину мережі, але й підвищує її надійність.

Логічну структуризацію виконують з метою підвищення продуктивності і безпеки даних шляхом розбиття єдиного для всієї мережі фізичного середовища на окремі сегменти за допомогою мостів, комутаторів і маршрутизаторів. Логічна структуризація дозволяє локалізувати трафік окремих сегментів і забезпечує одночасний обмін даними між комп'ютерами у межах кожного сегменту. Логічна структуризація не тільки підвищує ефективність мережі, але і зменшує можливість несанкціонованого доступу до даних.

До основних апаратних комунікаційних засобів локальних мереж відносяться мережеві адаптери (карти), повторювачі, концентратори, мости, комутатори, шлюзи і маршрутизатори. Мережеві адаптери призначені для під'єднання комп'ютерів до кабельної системи мережі і підтримують протоколи

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

канального та фізичного рівнів певної мережевої технології. Кожний мережевий адаптер має свою унікальну MAC-адресу, яка автоматично присвоюється комп'ютером, який використовує цей адаптер.

Для з'єднання двох сегментів фізичного середовища та відновлення якості (характеристик) електричних сигналів використовують такий комутаційний пристрій, як повторювач. Використання повторювача дозволяє виконати фізичну структурування побудованої на коаксіальному кабелі мережі, подвоїти її довжину, а також збільшити число під'єднаних до неї комп'ютерів.

1.2 Технології побудови локальних комп'ютерних мереж

Локальні комп'ютерні мережі будуються згідно з вимогами певної базової технології. Базова технологія локальної мережі ґрунтується на наборі стандартних протоколів і апаратно-програмних засобів, які ці протоколи реалізують. Стандарти базових технологій LAN висувають вимоги до структури та параметрів мережі, описують формати та алгоритми передавання даних, апаратно-програмні засоби їх реалізації, правил експлуатації і т.д. (аж до типу роз'ємів і способу використання проводів кабелю). Технологія може мати декілька специфікацій, які описують побудову різних варіантів мережі, наприклад, використання різного фізичного середовища. Найбільш поширеними базовими технологіями локальних мереж є Ethernet, Token Ring, FDDI, 100VG та ін. Формальними ознаками технологій побудови локальних комп'ютерних мереж є:

1. Метод доступу до фізичного середовища – процедура отримання права на передачу даних у фізичне середовище.
2. Формат повідомлень та алгоритми обміну ними.
3. Швидкість передавання даних.
4. Тип фізичного середовища, по якому передаються дані.
5. Топологія – спосіб з'єднання комп'ютерів між собою.
6. Діаметр мережі – віддаль між найбільш віддаленими комп'ютерами.
7. Максимальне число комп'ютерів.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

Алгоритм доступу до розділеного простору є одним із головних факторів, які визначають ефективність спільного використання середовища кінцевими вузлами локальної мережі. Можна сказати, що алгоритм доступу формує «вигляд» технології, який дозволяє відрізнити дану технологію від інших.

Основними технологіями, що використовуються для побудови локальних мереж, є Ethernet, Token Ring та FDDI.

В технології Ethernet застосовується дуже простий алгоритм доступу, який дозволяє вузлу мережі передавати дані у ті моменти часу, коли він вважає, що розділене середовище вільне. Простота технології Ethernet визначила простоту та низьку вартість обладнання Ethernet. Негативним атрибутом алгоритму доступу технології Ethernet є колізії, тобто ситуації, коли кадри, що передаються різними станціями, зіштовхуються одне з одним у загальному середовищі. Колізії знижують ефективність розділеного середовища та надають роботі з мережею непередбачуваного характеру.

Початковий варіант технології Ethernet був розрахований на коаксіальний кабель, який використовувався всіма вузлами мережі в якості загальної шини. Перехід на кабельні системи на витій парі та концентраторах (хабах) суттєво підвищив експлуатаційні характеристики мереж Ethernet. В технології Token Ring та FDDI підтримувались більш складні та ефективні алгоритми доступу до середовища, засновані на передачі одне одному токєну – спеціального кадру, який дозволяє доступ. Однак цієї переваги не було достатньо для успішного конкурування з технологією Ethernet.

1.3 Мережева технологія Ethernet

Однією з базових технологій локальних комп'ютерних мереж з комутацією пакетів є технологія Ethernet. Ця технологія використовує протокол CSMA/CD (множинний доступ з контролем що несе та виявленням колізій). Цей протокол дозволяє в кожний момент часу лише один сеанс передачі в логічному сегменті мережі. При появі двох і більше сеансів передачі одночасно виникає колізія, яка фіксується станцією, що ініціює передачу. Станція аварійно зупиняє процес і

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

очікує закінчення поточного сеансу передачі, а потім знову намагається повторити передачу.

Для передачі даних технологія Ethernet може використовувати:

- коаксіальний кабель з діаметром 0,5 дюйма, «товстий» коаксіал – стандарт 10Base-5;
- коаксіальний кабель з діаметром 0,25 дюйма, «тонкий» коаксіал – стандарт 10Base-2;
- неекранована вита пара (UTP, Unshielded Twisted Pair) – стандарт 10Base-T;
- оптоволоконний кабель – стандарт 10Base-F.

Дана технологія лежить в основі декількох швидкісних технологій: Fast Ethernet (100 Мбіт/с), Gigabit Ethernet (1000 Мбіт/с), 10 Gigabit Ethernet (10 Гбіт/с). На цей час розробляється технологія 100 Gigabit Ethernet з досягненням швидкості 100 Гбіт/с.

На цей момент для побудови локальних мереж використовують кабель витой пари. В рамках стандарту Ethernet створені специфікації 10BaseT, що використовує дві неекрановані виті пари UTP (Unshielded Twisted Pair) 3,4 або 5 категорій, та 100BaseT4, що ґрунтується на чотирьох витих парах UTP 5 категорії або екранованій витій парі STP (Shielded Twisted Pair). Для зв'язку між вузлами мережі необхідними є дві виті пари провідників: одна – для передавання, інша – для приймання інформації. Звичайно, замість двох кабелів по одній парі витих провідників у кожній використовують один кабель з чотирма парами провідників. Окрім економії та технічних переваг, це створює можливість переходу на більш швидкісні мережні архітектури без заміни самого кабелю.

Фізичні топології, що використовуються в технології Ethernet – «загальна шина» та «зірка». CSMA/CD (Carrier-Sense-Multiply-Access with Collision Detection) – метод колективного доступу з виявленням що несе та колізій. В мережах Ethernet комп'ютери підключені до спільного середовища передачі даних у вигляді гірлянди на новорічній ялинці. Тому в певний момент часу обмінюватись інформацією можуть лише два комп'ютери. Якщо в момент

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

обміну даними ще один комп'ютер спробує передати дані по загальній шині, то може виникнути колізія. Але дану проблему вирішує протокол CSMA/CD.

Всі комп'ютери в мережі мають можливість негайно (з урахуванням затримки розповсюдження сигналу у фізичному середовищі) отримати дані, які будь-який з комп'ютерів почав передавати у спільне середовище. Кажуть, що середовище, до якого підключені всі станції, працює в режимі колективного доступу (Multiply Access, MA).

Для отримання можливості передати кадр, інтерфейс-відправник повинен пересвідчитись у тому, що виділене середовище вільне. Це досягається завдяки прослуховуванню основної гармоніки сигналу, яка називається несучою частотою (Carrier Sense, CS). Ознакою «незайнятості» середовища є відсутність в ній носія частоти, яка при манчестерському способі кодування дорівнює 5-10 МГц залежно від послідовності нулів та одиниць, які передаються в цю хвилину. Якщо середовище вільне, то вузол має право на передачу кадру (рисунок 1.2). Кадр даних завжди супроводжується преамбулою, яка складається з 7 байтів, кожен з яких має значення 10101010, та 8 байту, рівного 10101011. Останній байт має назву обмежувача початку кадру. Преамбула необхідна для входження приймача в побітову та побайтову синхронізацію з передавачем. Наявність двох одиниць, що йдуть поруч, говорить приймачу про те, що преамбула закінчилась та наступний біт є початком кадру.

Всі станції, що підключені до кабелю, починають записувати байти кадру, що передається, у свої внутрішні буфери. Перші 6 байтів кадру містять адресу призначення. Та станція, яка визначила свою адресу в заголовку кадру, продовжує записувати його вміст у свій власний буфер, а інші станції на цьому приймання кадру зупиняють. Станція призначення оброблює отримані дані та передає їх верх по своєму стеку. Кадр Ethernet містить не лише адресу призначення, але і адресу відправника даних, тому станція-отримувач знає, кому потрібно відсилати відповідь.

Після закінчення передачі кадру всі вузли мережі зобов'язані дотримуватись технологічної паузи, яка рівна міжпакетному інтервалу (Inter Packet Gap, IGP) в

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

9,6 мкс. Ця пауза необхідна для приведення мережевих адаптерів у вихідний стан, а також для запобігання монопольного захоплення середовища однією станцією. Після закінчення технологічної паузи вузли мають право почати передачу свого кадру, оскільки середовище вільне.

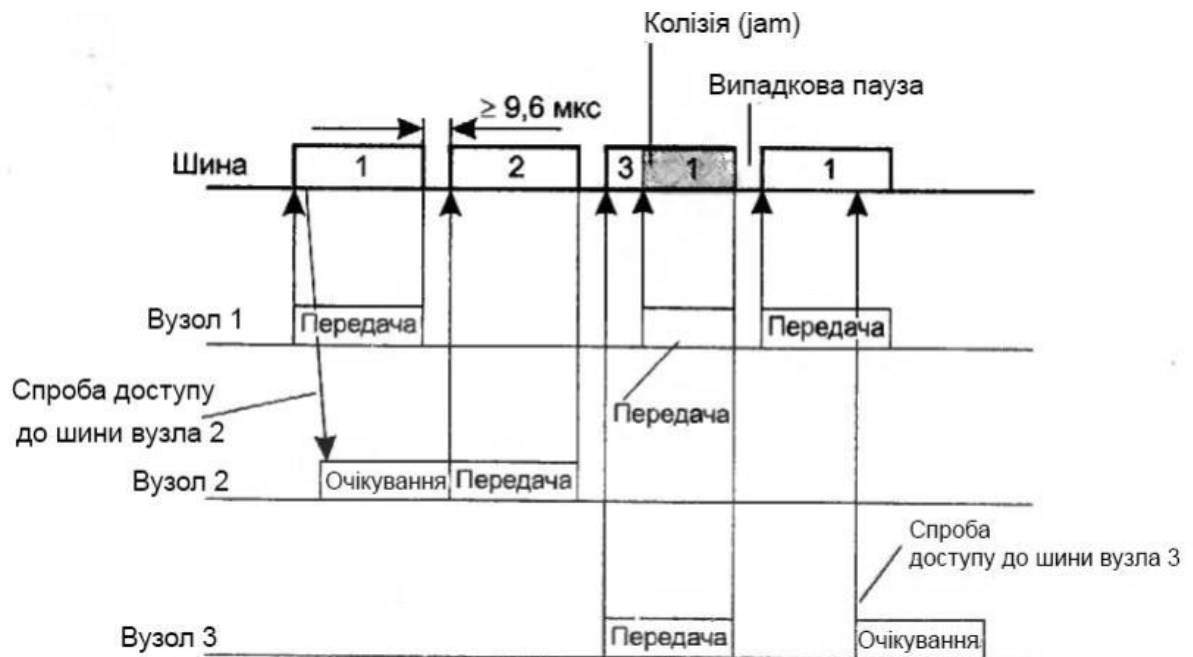


Рисунок 1.1 – Метод випадкового доступу CSMA/CD

Механізм прослуховування середовища та пауза між кадрами не гарантує виключення ситуацій, коли дві або більше станцій одночасно вирішують, що середовище вільне, та починають передавати свої кадри. Кажуть, що при цьому виникають колізії, оскільки вміст обох кадрів зіштовхуються у спільному кабелі та виникає спотворення інформації.

Для виникнення колізій не обов'язково, щоб декілька станцій почали передачу абсолютно одночасно, така ситуація малоімовірна. Більш вірогідна ситуація, коли один вузол починає передачу, а через деякий час (доволі короткий період) другий вузол, перевіривши середовище та не знайшовши носійний (сигнали першого вузла ще не встигли дійти до нього), починає передачу свого кадру. Таким чином, виникнення колізій є результатом розподілення вузлів мережі у просторі.

Для коректної обробки колізій всі станції одночасно спостерігають за утворювання в кабелі сигналів. Якщо сигнали, що передаються та

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

спостерігаються, відрізняються, то фіксується факт виникнення колізій (Collision Detection, CD). Для підвищення вірогідності найшвидшого виявлення колізій всіма станціями мережі, станція, що виявила колізію, перериває передачу свого кадру (у довільному місті, можливо, не на границі байта) та посилює колізію посилкою в мережу спеціальної послідовності із 32 біт, яка називається jam-послідовність.

Після цього передавальна станція, що виявила колізію, зобов'язана зупинити передачу та зробити паузу протягом короткого випадкового інтервалу часу. Потім вона може знову спробувати захопити середовище та передати кадр. Випадкова пауза вибирається за наступним алгоритмом:

$$\text{Пауза} = L * (\text{інтервал відтермінування}), \quad (1.1)$$

В технології Ethernet інтервал відтермінування обраний рівним значенню 512 бітових інтервалів. Бітовий інтервал відповідає часу між появою двох послідовних бітів даних на кабелі: для швидкості 10 Мбіт/с величина бітового інтервалу дорівнює 0,1 мкс або 100 нс [6]. L являє собою ціле число, вибране з рівною вірогідністю з діапазону $[0, 2N]$, де N – номер повторної спроби передачі даного кадру: 1, 2, ... 10.

Після 10-ї спроби інтервал, з якого вибирається пауза, не збільшується. Якщо 16 послідовних спроб передачі кадру викликає колізію, то передавач повинен припинити спроби та відкинути цей кадр. Описаний алгоритм має назву усіченого експоненціального двійкового алгоритму відстрочки.

1.4 Огляд та порівняння бездротових технологій

В цей час, що характеризується інформаційними проривами і активним використанням нових способів і методів передачі інформації, набули широкого поширення бездротові технології обміну даними з відповідними пристроями для реалізації точок входу, які можуть створювати віртуальні мережі. Протягом ряду років протікав процес стандартизації бездротової технології, збільшувалася швидкість передачі даних. Сьогодні вони дозволяють надавати підключення там, де неможливо кабельне з'єднання або потрібна повна мобільність.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

При цьому потрібно зазначити, сумісність бездротових мереж з кабельними.

Бездротові технології – це інформаційні технології, призначені для бездротової передачі інформації на відстані між двома і більше об'єктами [1-3]. Інформація може передаватися з використанням інфрачервоного випромінювання, радіохвиль, оптичного або лазерного випромінювання. На сьогодні розроблено вже велика кількість бездротових технологій, відомих по своїм маркетинговими назвами, наприклад, Bluetooth, WiMAX, Wi-Fi і інші [4-7]. Кожна технологія має певні характеристики, які визначають сферу її застосування.

Всі бездротові технології передачі даних підтримують як режим ad-hoc (настройка роботи без використання точки доступу), так і режим інфраструктури (підключення через точку доступу). При цьому передбачена можливість додавання нових користувачів в будь-який час і установки нових вузлів мережі в будь-якому місці без застосування мережевих шнурів. Де б не знаходилася точка доступу, абонентський комплект не прив'язаний до провідної комп'ютерної мережі. Робоча станція знаходиться завжди в мережі, що робить необов'язковим підключення мережевого шнура. Можна пересуватися по області, де є покриття і постійно залишатися підключеним до мережі [8-16].

Бездротові технології принципово змінюють соціальну структуру суспільства, моделі державного управління і механізми функціонування економіки, трансформують оборонні пріоритети і повсякденне життя громадян. Згідно з прогнозами Міжнародного союзу електрозв'язку, до 2020 року з використанням бездротових технологій кількість приєднаних до мережі пристроїв буде більш ніж в 6 разів перевищувати кількість підключених до мережі користувачів (25,5 млрд. Пристроїв проти 4 млрд. «Підключених» людей).

Стрімкий розвиток бездротових технологій, пов'язане з поширенням «блокнотних» комп'ютерів і інструментів пошукового виклику, популяризацією систем типу «персональний секретар» (Personal Digital Assistant «PDA»), а також розширення функціональних можливостей мобільних телефонів, дозволяє

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

віднести їх до найбільш швидко прогресує галуззю телекомунікацій, про що свідчать, наприклад, дати розробки і впровадження принципово нових стандартів і технологій.

Успіхи сучасної радіоелектроніки, розвиток мікропроцесорної техніки і нові алгоритми цифрової обробки сигналів разом з використанням перспективних телекомунікаційних технологій відкривають нові можливості зі створення безпроводних систем зв'язку з виконанням жорстких вимог, що стосуються високої пропускної здатності і перешкодозахищеності. Такі системи покликані забезпечувати розрахунок часу, ділове планування, підтримку постійного зв'язку з віддаленими станціями, зберігання документів. Принципом бездротових технологій став вираз «Any time and any where», тобто надання послуг зв'язку незалежно від місця і часу. На сьогоднішній день найбільш відомими технологіями бездротового зв'язку є ZigBee, Bluetooth і звичайно ж Wi-Fi. При цьому кожна з цих технологій є ефективною в різних сферах і ситуаціях, розглянемо їх більш детально, виділимо переваги і недоліки, а також проаналізуємо в яких сферах діяльності вони найбільш ефективні.

1.5 Технологія бездротової передачі даних Wi-Fi

Технологія Wi-Fi, або Radio Ethernet IEEE 802.11 – є першим промисловим стандартом, який дозволив організувати бездротову локальну мережу (Wireless Local Area Networks – WLAN) на обмеженій території, тобто коли кілька користувачів мають рівний доступ до загального каналу передачі даних.

Стандарт був створений в Інженерному інституті електротехніки та радіо електроніки (Institute Electrical and Electronics Engineers – IEEE) і може зрівнятися зі стандартом 802.3 для звичайних дріт'яних Ethernet мереж. Центром бездротової мережі WI-FI є точка доступу (Access Point), яка може підключатися до будь-якої наземної мережевої інфраструктури, наприклад, офісної Ethernet-мережі і забезпечувати передачу радіосигналу.

На сьогоднішній день розроблено вже безліч версій стандарту – IEEE 802.11 з відповідними літерними індексами a, b, c, d, e, g, h, i, j, k, l, m, n, o, p, q, r, s, u,

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

v, w. Однак тільки чотири з них (a, b, g і n) є найбільш поширеними і популярними у виробників обладнання, інші ж являють собою удосконалення, доповнення або виправлення вже прийнятих специфікацій. Перша специфікація стандарту IEEE 802.11 була прийнята в 1997 році. Вона встановила передачу даних на швидкості 1 і 2 Мбіт/с в неліцензійному діапазоні частот 2,4 ГГц, а також механізм управління доступом до фізичного середовища (радіоканалу), який використовує метод множинного доступу з розпізнаванням що несе і усуненням колізій (Carrier Sense Multiple Access with Collision Avoidance, CSMA-CA). У таблиці 1.1 представлені ключові технічні характеристики основних стандартів IEEE 802.11.

Таблиця 1.1

Ключові характеристики основних стандартів IEEE 802.11

Стандарт	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
Рік ратифікації Wi-Fi альянсом	1999	1999	2003	2009
Частотний діапазон	5.15-5.24 5.67-5.85	2.4-2.482	2.4-2.483	2.4-2.481 5.15-5.24 5.67-5.85
Доступ до радіоканалу	CSMA-,CA	CSMA-,CA	CSMA-,CA	CSMA-,CA
Кількість абонентів на один канал	64	64	64	64
Максимальна швидкість обміну даних	54 Мбіт/с	11 Мбіт/с	54 Мбіт/с	600 Мбіт/с
Звичайна швидкість передачі даних	23 Мбіт/с	4 Мбіт/с	20 Мбіт/с	120 Мбіт/с
Ширина каналу	20 МГц	22 МГц	20 МГц	40 МГц
Метод модуляції	OFDM	BPSK, CCK	OFDM	BPSK, QPSK, 16-QAM 64-QAM
Дальність дії в приміщенні	10-20	20-100	20-50	10-20

Одночасно потрібно зазначити, що Міжнародна організація Wi-Fi Alliance презентувала новий стандарт бездротового зв'язку Wi-Fi 802.11ah «Ha Low». Діапазон роботи нового стандарту 900 МГц, саме на цій частоті пристрої Wi-Fi Certified можуть підключатися на більшій відстані з найменшими витратами енергії. За радіусом дії Wi-Fi «HaLow» приблизно у два рази перевершує використовувані в цей час варіанти Wi-Fi. Крім того, діапазон 900 МГц надає можливості, які необхідні для таких додатків, як мобільні електронні пристрої і датчики, які користувачі носять з собою.

На відміну від уже прийнятих стандартів, які працюють на частоті у 2,4 ГГц і 5 ГГц, Wi-Fi 802.11ah подвоює радіус дії сигналу, забезпечує надійне з'єднання, в разі, якщо радіохвилі проникають через перешкоди, наприклад, стіни (див. Рис .1.1). Окремо потрібно звернути увагу на той факт, що, у зв'язку з альтернативної частоти, новий стандарт не схильний до перешкод від мікрохвильових печей і інших побутових приладів.

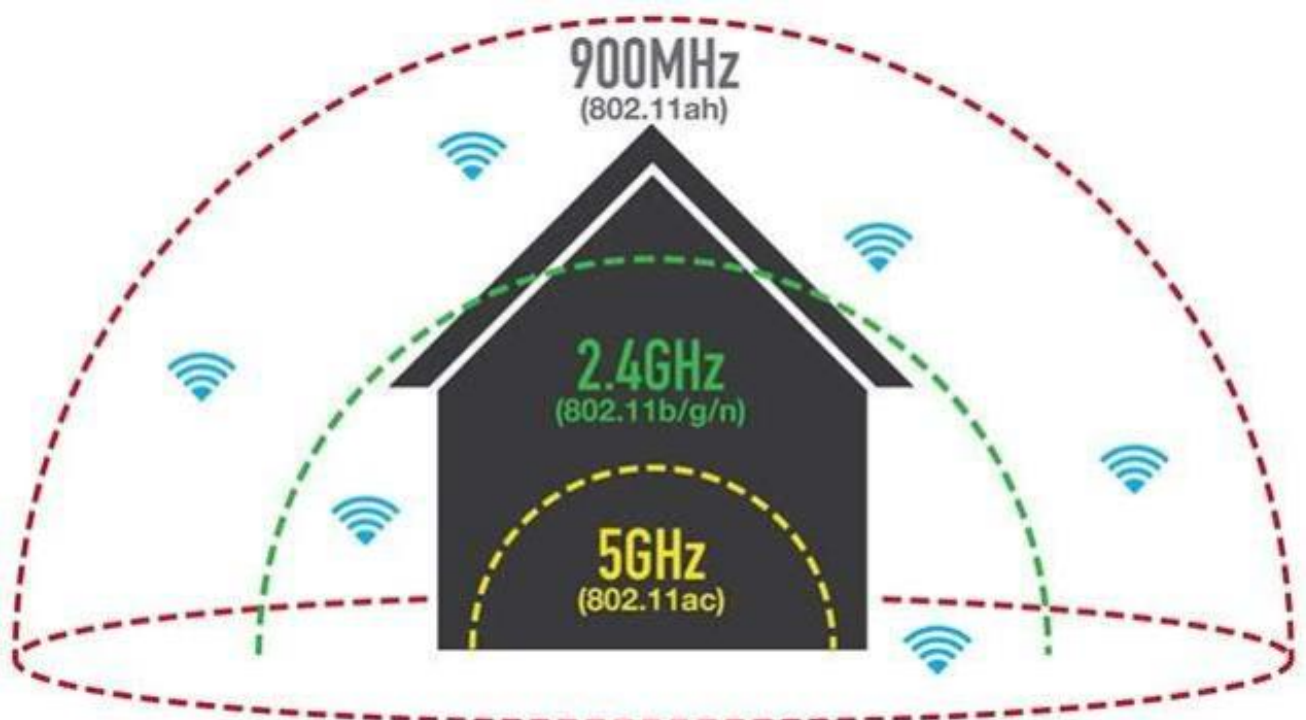


Рисунок 1.2 – Діапазон дії нового стандарту бездротового зв'язку Wi-Fi 802.11ah «HaLow».

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

Розробники запевняють, що Wi-Fi 802.11ah буде володіти всіма перевагами Wi-Fi, включаючи простоту установки, широку сумісність обладнання, а також надійний захист даних. Крім того, планується, що пристрої, з підтримкою Wi-Fi «HaLow» також будуть працювати в діапазонах 2,4 і 5 ГГц, це дозволить їм інтегруватися в чинну екосистему Wi-Fi, до якої входить понад 7 млрд.

Пристроїв. Аналогічно пристроїв Wi-Fi, пристрої Wi-Fi «HaLow» будуть підтримувати підключення по IP, завдяки чому вони зможуть працювати з хмарними сервісами, що має велике значення і важливість для інтернету і збережених в ньому речей. Ще одне безперечна перевага Wi-Fi «HaLow» полягає в можливості підключення до однієї точки доступу тисяч пристроїв.

Крім нового стандарту Wi-Fi 802.11ah ключові перспективи розвитку Wi-Fi найближчим часом полягають в наступному:

- освоєння діапазону 60 ГГц. Wireless Gigabit Alliance (WiGig Alliance) розвиває технологію Wi-Fi в діапазоні 60 ГГц з максимальною швидкістю передачі 7 Гбіт / с для сценаріїв піко-клітинного покриття;
- розвиток технології Wi-Fi Direct, яка дозволяє забезпечити зі звичайною швидкістю Wi-Fi прямі з'єднання між різними клієнтськими пристроями, обходячи традиційні точки доступу і бездротові маршрутизатори;
- підтримка вдосконалених рішень VoIP з оновленим набором WFA-протоколів для розвитку конкурентоспроможних альтернативних послуг;
- розвиток стільникових (Mesh) Wi-Fi мереж, заснованих на дешевих модулях, кожен з яких по радіоканалу з'єднаний з усіма сусідами в зоні радіовидимості;
- подальше вдосконалення радіо інтерфейсу Wi-Fi;
- удосконалення клієнтського досвіду Wi-Fi за допомогою оптимізації взаємодії з точками доступу.

І в завершенні аналізу технології бездротової передачі даних Wi-Fi відзначимо, що її основні переваги полягають в:

- простоті використання готових модулів;
- легкості інтеграції з чинними провідними мережами (LAN);

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

- високій швидкості передачі інформації;
- більш високою (у порівнянні з іншими бездротовими мережами) ціною на обладнання;
- великим (в порівнянні з іншими бездротовими мережами) енергоспоживанням;
- роботою безлічі пристроїв в діапазоні частот 2.4 ГГц, наприклад, мають Bluetooth адаптер, це погіршує якість передачі інформації;
- наявний в кожній країні експлуатаційними обмеженнями і частотними діапазонами;
- недостатньо захищеним стандартом шифрування WEP, який використовується для захисту доступу до мережі.

Розглядаючи більш детально сфери застосування технології бездротової передачі даних Wi-Fi, можна відзначити, що сьогодні вона використовується в багатьох областях діяльності. Найбільший попит технологія отримала в Інтернет-провайдерів, оскільки це дозволяє їм відмовитися від десятків кілометрів проводів.

Також дана технологія використовується в ігровій індустрії. Такі відомі бренди як Sony і Nintendo монтують Wi-Fi пристрої у свої ігрові консолі, для забезпечення доступу до Інтернету. Деякі комерційні організації надають доступ до мережі Інтернет з використанням даної технології. Якщо ж розглядати великі компанії і корпорації, то вони використовують Wi-Fi для створення корпоративної мережі, оскільки це дешевше ніж створювати дротову мережу Ethernet.

1.6 Основні принципи побудови і функціонування мереж IEEE 802.11

Впровадження технології бездротового ширококутового доступу, заснованої на специфікаціях IEEE серії 802.11 (Wi-Fi), як уже зазначалося раніше, може забезпечити потреби користувачів не тільки в ширококутовий доступ до

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

Інтернету, а й в частині передачі даних поперх Wi-Fi. Крім того, Wi-Fi надає можливості для побудови цільових мереж, що може сприяти розширенню клієнтської бази та надання користувачам принципово нових послуг. Все це можливо за умови коректного і ефективної побудови самої мережі.

Як свідчить проведений науковий аналіз і спеціалізованих робіт з даної проблематики, В цей час дослідження в області бездротових технологій стандарту 802.11 набувають все більшого поширення. Це пов'язано з тим, що апаратні засоби і протоколи, що лежать в основі таких мереж, є досить новими і швидко розвиваються.

Велика увага аналізу та вирішення проблем розробки надійних бездротових мереж, в тому числі і стандарту IEEE 802.11, а також створення програмних і апаратних засобів для них, приділяють провідні компанії в області виробництва радіоелектронних компонентів, а саме Digi, Freescale, Semiconductor, Ember, Texas Instruments і т.д. В цей час дослідження в цій області ведуться в основному по розробці нових протоколів зв'язку.

У науковій сфері можна відзначити наступні напрацювання. Так, наприклад, в роботах представлені основні характеристики бездротових систем і приведено загальний вираз для потужності приймального сигналу. Поряд з дослідженнями стандартів 802.11 проводяться дослідження стандарту 802.16. Ці стандарти схожі між собою, а також для них характерна наявність однакових типів перешкод в середовищі передачі. У роботах були оцінені причини і наведені методи боротьби з між каналного інтерференційними перешкодами для багатопозиційних сигналів. В результаті чого було встановлено, що при використанні великої кількості піднесуть, збільшується швидкість передачі в каналі, а також збільшуються вимоги до параметра сигнал / шум. Одним із вагомих чинників, який необхідно враховувати, є тип модуляції. У стандарті 802.11 використовується два види модуляції MPSK для низько швидкісної передачі і QPSK для високошвидкісної передачі. як показують дослідження одним з критеріїв ефективності передачі інформації є забезпечення відповідного рівня сигнал / шум.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Не викликає сумніву той факт, що ключовий параметр, який характеризує будь-який канал передачі – це пропускна здатність. Саме забезпечення цього параметра в певних межах і можливості його підвищення, свідчать про ефективність роботи каналу. З іншого боку, розглядаючи бездротові канали стандарту 802.11 Wi-Fi, можна спостерігати невеликий виділений частотний ресурс, на якому розміщується велика кількість мереж, що використовують однакові канали для передачі інформації. Особливо це стосується областей з високою складністю забудови і щільністю населення (кількість мереж може досягати більше 50). В такому випадку, при збігу частотних каналів, інформаційні пакети кожної мережі займають тимчасові проміжки між пакетами іншої мережі.

Всі ці фактори призводять до виникнення перешкод і зменшення параметра корисної пропускної здатності. Таким чином, з урахуванням вищевикладеного, представляється доцільним з метою визначення ефективних принципів побудови і формалізації структури бездротового каналу стандарту 802.11 з урахуванням максимально можливої кількості чинників, які впливають на характеристики передачі, докладно розглянути, що являє собою стандарт IEEE 802.11 як базовий для всіх наступних специфікацій.

Як і всі стандарти комітету IEEE 802, в документі IEEE 802.11 розглядаються два нижніх рівні моделі взаємодії відкритих систем (OSI): фізичний і канальний (Data Link layer). Причому останній підрозділяється на два підрівні. Верхній – Logical Link Control (LLC) – описаний в стандарті IEEE 802.2. Стандарт IEEE 802.11 розглядає тільки нижній підрівень – Medium Access Control (MAC), тобто управління доступом до каналу (середовищі передачі). Іншими словами, на фізичному рівні стандарт визначив спосіб роботи з середовищем передачі, швидкість і методи модуляції. На MAC-рівні – принцип, за яким пристрої використовують (ділять) загальний канал, способи підключення пристроїв до точок доступу і автентифікації, механізми захисту даних.

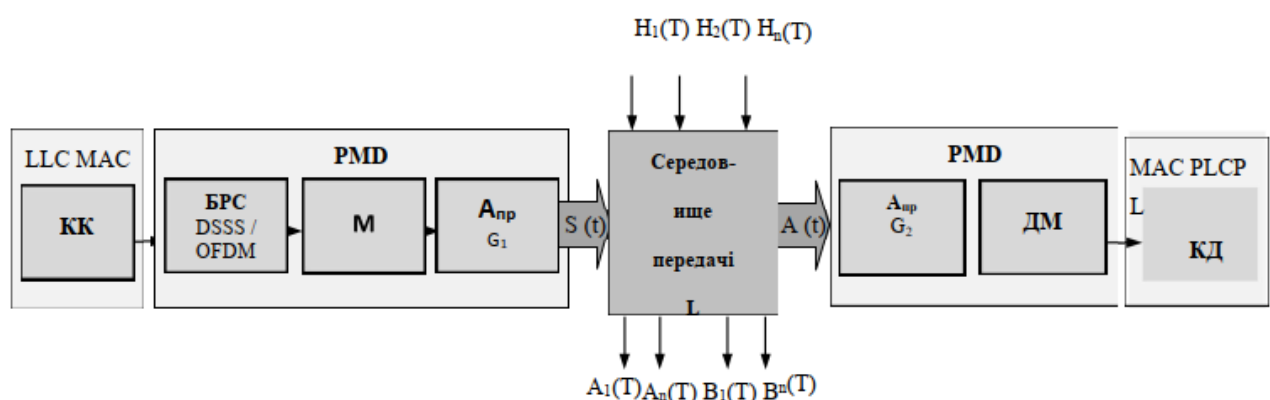
Оскільки стандарт IEEE 802.11 розроблявся як «бездротової Ethernet», він передбачає пакетну передачу з 48-бітними адресами пакетів, як і будь-яка

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

мережа Ethernet. Комітет IEEE 802 особливу увагу приділяв сумісності всіх своїх стандартів, в результаті провідні та безпроводні мережі IEEE 802 легко поєднуються один з одним.

З точки зору побудови бездротових Wi-Fi мереж, канали передачі для аналізу можна уявити, як точки доступу і абонентські адаптери і інтерфейси. Кожне таке пристрій містить як передавач, так і приймач, які виконують обмін радіосигналами через середу передачі, а також виконують роль перетворювачів інформації від мережевих інтерфейсів в радіосигнали і навпаки.

У найпростішому випадку побудова бездротового каналу передачі, можна розглянути, як пару – передавач і приймач, що показано на рисунку 1.3. На каналному рівні (підрівні LLC і MAC) і підрівні PLCP виконується завадостійке кодування, так званим каналним кодером (КК). Тут виконується формування кадру PPDU, який вміщує в себе службову і корисну інформацію для передачі.



$B_1(t), \dots, B_n(t)$ -перешкоди, які мають природний характер, перешкоди від пристроїв інших систем передачі і побутових приладів;

$A_1(T), \dots, A_n(T)$ - Перешкоди, які вносять інші передавачі стандарту Wi-Fi;

$H_1(T), \dots, H_n(T)$ - Інтерференційні перешкоди.

Рисунок 1.3 – Структура бездротового каналу стандарту Wi-Fi.

Підрівень PMD каналного рівня, перетворює двійкову послідовність в модульоване ВЧ-коливання за допомогою квадратурного модулятора (М) і блоку

розширення спектра (BPS). Для стандартів 802.11 n і вище використовується OFDM, а для нижчих – DSSS. На виході передавальної антени ($A_{пр}$) формується сигнал $S(t)$ і надходить в середу передачі. Потужність сигналу передавача є заздалегідь визначеною величиною і становить для стандарту Wi-Fi 100 мВт. Поряд з цим значенням внутрішні шуми електричних ланцюгів передавача є незначними і ними можна знехтувати. Основні перешкоди, що призводять до зміни і загасання сигналу, діють в середовищі передачі.

Розглядаючи на наступному етапі радіо тракт, не можна обійти увагою ключове питання – частотний діапазон. IEEE 802.11 прив'язаний до чинних в США і ряді інших країн без ліцензійних частотних діапазонів. Спочатку він був орієнтований на діапазон 2,400-2,4835 ГГц з шириною смуги 83,5 МГц. Обумовлена стандартом спектральна маска для одного каналу приведена на рисунку 1.5 (потужність відраховується щодо піків функції $\sin(x)/x$). Ширина каналу на рівні – 30 дБ становить 22 МГц, отже, в смузі 83,5 МГц можливо три канали, які не перекриваються.

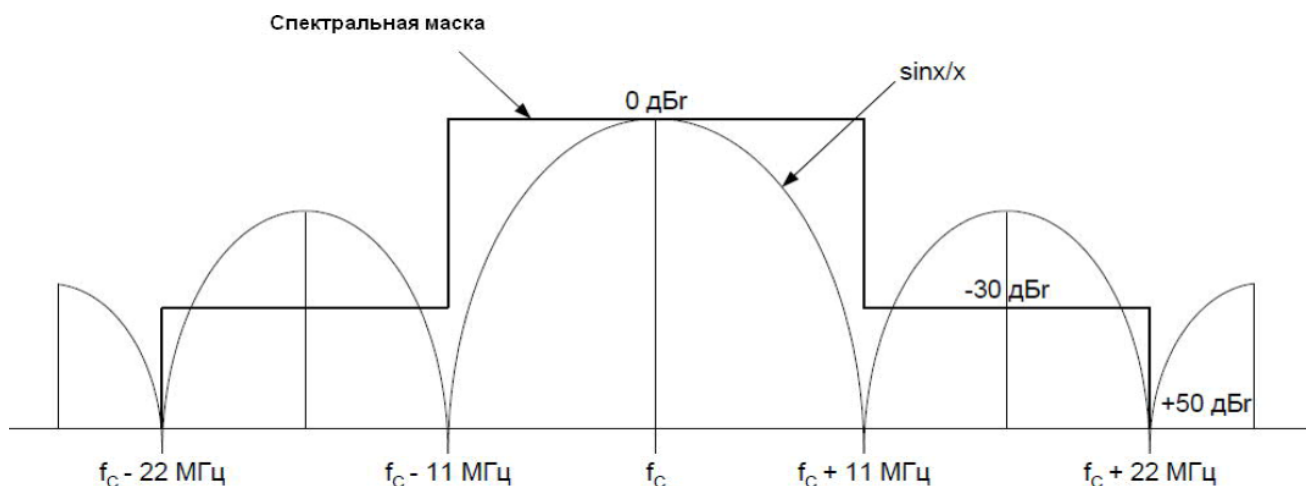


Рисунок 1.4 – Спектральна маска каналу мережі 802.11.

Стандарт IEEE802.11 передбачає два основних способи організації локальної мережі: за принципом «рівний з рівним» (ad-hoc-мережа – рисунок 1.6.3, а) і у вигляді структурованої мережі (рисунок 1.6.3, б).

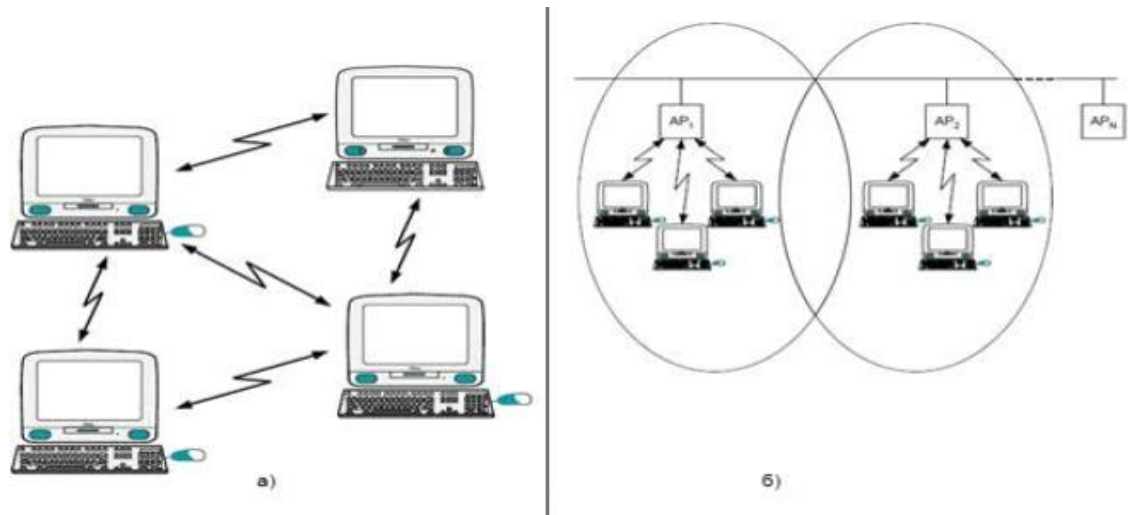


Рисунок 1.5 – Архітектура мережі 802.11: а - Ad-hoc-мережа; б – Структуровані мережі.

У першому випадку, а) зв'язок встановлюється безпосередньо між двома станціями, і ніякого адміністрування не передбачено. У разі структурованих мереж (а, як показала практика, це основний спосіб побудови мереж IEEE 802.11) в їх складі з'являється додатковий пристрій – точка доступу (AP - Access Point), як правило, стаціонарна і що діє на фіксованому каналі. Зв'язок між пристроями відбувається тільки через AP. Через них же можливий вихід в зовнішні провідні мережі.

У мережі IEEE 802.11 може бути кілька AP, об'єднаних провідною мережею Ethernet. Фактично така мережа являє собою набір базових станцій з зонами охоплення, що перекриваються. Стандарт IEEE 802.11 допускає переміщення пристроїв з однієї зони AP в іншу (роумінг), тим самим забезпечуючи мобільність.

Оскільки для мобільних станцій важливим є питання ресурсу елементів живлення, в стандарті закладено спеціальний протокол управління енергоспоживанням – безпосередньо при обміні передавальний пристрій може перевести приймач в режим очікування.

Крім того, при побудові мережі IEEE 802.11 важливі є ряд таких моментів. По-перше, це вибір стандарту бездротової мережі. Порівняння стандартів наведено в таблиці 1.1 Як свідчить дана таблиця, безсумнівні переваги має

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

стандарт IEEE 802.11n, до числа яких відносяться: збільшення швидкості передачі даних; збільшення зони покриття; збільшення надійності передачі сигналу; збільшення пропускної здатності. На фізичному рівні стандарту реалізована вдосконалена обробка сигналу і модуляції, додана можливість одночасної передачі сигналу через чотири антени. На мережному рівні реалізовано більш ефективне використання доступної пропускної здатності. Разом ці вдосконалення дозволяють збільшити теоретичну швидкість передачі даних до 600 Мбіт / с, що більше ніж в десять разів більше, в порівнянні з 54 Мбіт / с стандарту 802.11a / g.

По-друге, потрібно визначитися з методом об'єднання всіх елементів бездротової мережі. Завдання полягає в тому, щоб всі мобільні пристрої в підконтрольній зоні мали можливість передавати і отримувати дані від бездротової мережі. При цьому повинен дотримуватися принцип, при якому переміщення мобільного пристрою з однієї зони покриття Wi-Fi в іншу зону для користувача буде непомітно, тобто не потрібно було вручну робити повторне підключення і вводити пароль.

Основними режимами роботи точки доступу Wi-Fi є:

- режим точки доступу Access Point (AP);
- режим бездротового мосту Wireless Bridge;
- режим AP / Bridge (AP + Bridge);
- режим повторювача Repeater (Bridge / Repeater);
- режим роумінгу (Roaming);
- режим бездротової системи розподілу WDS (Wireless Distribution System).

По-третє, вибір обладнання. Різноманітність фірм виробників мережевих бездротових пристроїв величезна, а ще більше марок цих пристроїв. Необхідно чітко позначити критерії вибору і ключові моменти. Звісно ж, що при виборі обладнання в першу чергу слід звернути увагу на такі особливості:

- внутрішня або зовнішня точка доступу (в приміщенні / на вулиці);
- тип антени (спрямована, все спрямована);

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

- наявність портів (які роз'єми є в пристрої);
- які стандарти підтримує (IEEE 802.11);
- частотний діапазон;
- потужність бездротового сигналу;
- режими роботи;
- скільки користувачів одночасно підтримує одна точка доступу.

По-четверте, можливі втрати ефективності сигналу Wi-Fi після проходження різних перешкод (див. таблицю 1.2).

Таблиця 1.2

Втрата ефективності сигналу Wi-Fi при проходженні через різні середовища.

Перешкода	Додаткові втрати, дБ	Ефективна відстань, %
Відкритий простір	0	100
Вікно	3	70
Дерев'яна стіна	10	30
Міжкімнатні стіни завтовшки 15,2 см	15-20	15
Опорна стіна завтовшки 30,5 см	20-25	10
Бетонна підлога або стеля	15-25	10-15
Монолітне залізобетонне перекриття	20-25	10

Таким чином, підбиваючи підсумок, відзначимо, що в процесі проєктування бездротової мережі необхідно брати до уваги: стандарт зв'язку, спосіб об'єднання точок доступу, тип обладнання та зону покриття «Корисного» сигналу. Якщо один з чотирьох пунктів не врахований, то дальність дії сигналу скоротиться в багаторазовому розмірі.

Це, в свою чергу, буде сприяти появі затримок і помилок під час отримання доступу до послуг з великим обсягом трафіку. Тому, на сьогоднішній день видається актуальним пошук нових методів і засобів для мінімізації впливу вищенаведених факторів.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

Одне з таких напрямків – вдосконалення математичних моделей бездротових мереж і їх каналів, які здатні максимально враховувати особливості середовища передачі.

1.7 Особливості забезпечення захисту локальної мережі

Безпечна архітектура – це фундамент

Отже, крім централізованої політики безпеки, без якої de facto неможливо побудова безпечної мережі в принципі, особливу увагу слід звернути на таке:

Використання безпечних протоколів обміну (не секрет, що такі текстові протоколи, як FTP і Telnet, являють собою явну загрозу) і тунелювання даних, наприклад, за допомогою SSH;

Шифрування критичних даних з використанням надійних криптоалгоритмів;

Використання архітектури, що містить наявність DMZ (демілітаризованої зони), що обслуговується двома фаєрволами;

Використання IDS (Intrusion-Detection System), IPS (Intrusion-Prevention System) і NAT;

Захист периферії допомогою тонких клієнтів і двох факторної системи автентифікації.

DMZ. Проектування демілітаризованої зони

Не секрет, що системи, відкриті для прямого доступу ззовні, є головними цілями зловмисників. Для організацій, що мають справу з критичною та конфіденційною інформацією, питання захисту периметра мережі стоїть особливо гостро. Політика безпеки зовнішніх систем (web-сервер, поштовий сервер та інші) вимагають самого ретельного опрацювання, оскільки вони піддаються нападу в першу чергу. Завдання полягає в тому, щоб обмежити доступ цих систем до дійсно важливих і секретним комп'ютерам, розташованих усередині мережі, що реалізується за допомогою технологій, описаних мною нижче.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

DMZ – скорочення від demilitarized zone (демілітаризована зона) – являє собою фрагмент мережі, не є повністю надійним. Сенс створення DMZ полягає в тому, щоб відгородити внутрішню систему (в такому випадку це наша захищена LAN) від доступу, який здійснюється з Інтернету. DMZ створюється за допомогою реалізації напівзахищеної мережевої зони, що досягається шляхом застосування між мережевими екранів або маршрутизаторів зі строгими фільтрами. Потім за допомогою елементів керування мережею визначається політика, якого трафіку дозволяється проникнення в DMZ, а якому трафіку дозволено виходити за межі DMZ. Очевидно, що всі системи, доступні з зовнішнього середовища, повинні бути розміщені в демілітаризованій зоні. Слід враховувати й те, що, якщо система доступна через інтерактивний сеанс (такий, як telnet або SSH), то відкривається можливість проведення атак проти інших систем, що знаходяться в DMZ. В якості моделі розглянемо наступну. Одна з можливих архітектур безпечної LAN з використанням демілітаризованої зони.

В такій ситуації наша мережа містить два між мережевими екранів, що відокремлюють DMZ від зовнішньої і внутрішньої мережі. Зовнішня мережа виявляється між маршрутизатором провайдера і першим фаєрволом, в той час, як демілітаризована зона розміщується між мережевими екранами №1 і №2. У налаштуваннях між мережевого екрана №1 передбачено дозвіл проходження всього трафіку DMZ, а також всього внутрішнього трафіку (за деяким винятком). Між мережевий екран №2 налаштований більш жорстко з урахуванням того, що дозволено тільки вихідний інтернет-трафік. Подібна конфігурація значно підвищує загальний рівень безпеки LAN. Не можна не погодитися з тим, що використання і обслуговування пари між мережевими екранів підвищує вартість архітектури і вимагає додаткових зусиль з управління та налаштуванні, але... воно того варто.

IDS – система виявлення вторгнень. В ідеальному випадку така система лише видасть сигнал тривоги при спробі проникнення. Виявлення вторгнень допомагає при превентивної ідентифікації активних загроз за допомогою повідомлень і попереджень про те, що зловмисник здійснює збір інформації,

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

необхідної для проведення атаки. Різновидом IDS є IPS, можливості якої виходять за рамки простого виявлення вторгнень і доповнюються можливістю превентивної протидії. В цей час можна виділити принаймні два основних типи IDS:

- вузлові (HIDS);
- мережеві (NIDS).

Як правило, система HIDS розміщується у вузлах системи, відстежуючи будь-яку підозрілу активність, яку можна класифікувати як ознаки атак на даний вузол. HIDS являють собою систему датчиків, що завантажуються на різні сервери організації і керованих центральним диспетчером. Сенсор HIDS дозволяє визначити, чи була атака успішною, якщо атака мала місце на тій же платформі, на якій встановлено датчик. Слід зауважити, що система HIDS, як правило, коштує дорожче, ніж мережева система, що пояснюється тим, що кожен сервер повинен мати ліцензію на датчик (датчики дешевше для одного сервера, однак загальна вартість датчиків більше порівняно з вартістю використання мережевих IDS).

При використанні системи HIDS слід звернути увагу на те, що робота процесу датчика на сервері може займати до 15% загального процесорного часу. При активно використовуваній системі, подібна витрата системних ресурсів може негативно позначитися на продуктивності, і, таким чином, не виключено, що вам доведеться купувати більш продуктивну систему. NIDS являє собою програмний комплекс, що працює на спеціально виділеній системі.

Принцип функціонування NIDS чимось схожий з роботою мережного «сніфер»: NIDS переводить роботу мережевої карти в системі promiscuous mode (безладний режим – стан, у якому мережевий адаптер виявляє в мережі всі фрейми незалежно від їх кінцевої адреси). Після отримання пакетів відбувається аналіз трафіку з використанням набору правил та ознак атак для визначення того, чи становить цей трафік який-небудь інтерес. На рис. 2 показана можливість використання двох типів IDS:

NAT

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

Ще одним інструментом, який ми застосуємо при проектуванні безпечної LAN, стане NAT.

NAT – це технологія трансляції однієї чи кількох адрес в інші адреси. У більшості випадків функції NAT реалізуються за допомогою між мережевого екрана (хорошим прикладом є Kerio Win Rout Firewall з гнучкою системою налаштування NAT). Маршрутизатори також можуть виконувати цю функцію. Очевидно, що функція безпеки NAT реалізується завдяки тому, що приховані адреси внутрішніх систем є невидимими із зовнішньої мережі, зокрема мережі Інтернет. Слід враховувати і той факт, що для захисту від інсайдерських атак NAT марна: якщо зловмисник знаходиться всередині організації або має прямий доступ до внутрішньої мережі через VPN або телефонне з'єднання, то NAT і зовсім ніяк не зможе захистити мережу.

Необхідний мінімум:

При побудові безпечної LAN слід мінімізувати кількість служб і сервісів, що надаються мережею, що використовуються клієнтами з мережі Інтернет;

Архітектура LAN в обов'язковому порядку повинна передбачати наявність DMZ – демілітаризованої зони, контрольованої між мережевим екраном;

Вкрай бажано наявність NAT (система переадресації виконує функцію приховування адрес внутрішніх систем);

Установка останніх оновлень строго обов'язкова. Навіть якщо ваша система має найостанніші оновлення, розслаблятися все одно не варто: з моменту виявлення нової уразливості і до моменту виходу заплатки «розумні люди» встигають написати експлоїт або створити хробака;

Зрозуміло, як на сервері, так і на робочих станціях має бути встановлене антивірусне ПЗ зі свіжими базами;

Якщо у вас досі файлова система FAT32, змініть її на NTFS. NTFS de facto більш безпечна: вона дозволяє розмежувати доступ до ресурсів вашого ПК і значно ускладнить процес локального та мережного злому паролів бази SAM;

У властивостях підключення вкрай бажано залишити лише саме необхідне TCP/IP. «Службу доступу до файлів і принтерів у мережі Microsoft» необхідно

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

відключити (стосується машин, не надають SMS-доступ), щоб не полегшувати завдання всім любителям «дефолтові» C\$, D\$ ADMIN\$ і т. д.

Всі невживані сервіси бажано вимкнути. Це не тільки поліпшить продуктивність вашої системи, але і автоматично закриє купу відкритих портів;

Видаліть зайві облікові записи (такі, як HelpAssistant і SUPPORT_388945a0), а в оснащенні gpedit.msc забороніть локальний і мережевий вхід для всіх користувачів, залишивши тільки що використовуються на цій машині;

Користувача «Адміністратор» краще перейменувати (через оснастку gpedit.msc);

Відкриті за замовчуванням ресурси C\$, D\$ ADMIN\$ бажано відключити (створенням параметра DWORD за адресою HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \lanmanserver \parameters);

В локальній мережі не варто забувати і про снифферах, з допомогою яких ваші паролі можуть стати «суспільним надбанням» (не секрет, що паролі таких сервісів, як FTP і Telnet, передаються по LAN у відкритому вигляді). Використовуючи сниффер (наприклад, Cain&Abel), навіть зашифровані паролі легко зламати. Вихід – побудова локальної мережі не на хабах (мережеві пакети, які отримує хаб, розподіляються за всіма адресами незалежно від місця призначення), а на комутаторах (використовується технологія доставлення пакетів «за адресою»). Застосування комутаторів значно ускладнює процес перехоплення мережевих паролів і робить зловмисника «видимим» (перехоплення паролів можливий навіть при використанні комутаторів, але в цьому випадку машина зловмисника змушена генерувати ARP-пакети – технологія ARP-poizoning), використовуючи стандартний набір для антисниффінга;

Мінімальна мінімум сесії безпека має на увазі використання криптистійкого алгоритму – NTLMv2.

Використання NTLMv2-механізму замість уразливого LM або NT значно підвищує криптистійкість паролів (включається через оснастку «Локальні параметри безпеки») і знижує можливі ризики, пов'язані з перехопленням і

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

розшифровкою хешей. Перераховані способи захисту/побудови безпечної мережі – аж ніяк не панацея проти всіх, хто серйозно вирішив зламати вашу мережу. Дотримання перерахованого вище мінімуму значно знижує ймовірність злому, роблячи вашу мережу більш безпечною до зовнішніх і внутрішнім загрозам.

1.8 Особливості забезпечення захисту безпроводних мереж

Всі сучасні бездротові пристрої (точки доступу, бездротові адаптери і маршрутизатори) підтримують протокол безпеки WEP (Wired Equivalent Privacy), який був спочатку закладений в специфікацію бездротових мереж IEEE 802.11. Даний протокол є свого роду аналогом провідної безпеки, проте реально ніякого, еквівалентного провідним мережам рівня безпеки, він, звичайно ж, не забезпечує.

Протокол WEP дозволяє шифрувати потік переданих даних на основі алгоритму RC4 з ключем розміром 64 або 128 біт – ці ключі мають так звану статичну складову довжиною від 40 до 104 біт і додаткову динамічну складову розміром 24 біти, звану вектором ініціалізації (Initialization Vector, IV).

Процедура WEP-шифрування виглядає наступним чином. Спочатку передані в пакеті дані перевіряються на цілісність (алгоритм CRC-32), після чого контрольна сума (integrity check value, ICV) додається в службове поле заголовка пакета. Далі генерується 24-бітний вектор ініціалізації (IV), а до нього додається статичний (40 або 104-бітний) секретний ключ.

Отриманий таким чином 64 або 128-бітний ключ і є вихідним ключем для генерації псевдовипадкового числа, яке використовується для шифрування даних. Далі дані змішуються (шифруються) за допомогою логічної операції XOR з псевдовипадковою ключовою послідовністю, а вектор ініціалізації додається в службове поле кадру. Протокол WEP є далеко не найкращим способом захисту бездротової мережі. Після публічної демонстрації численних вразливостей WEP, IEEE розпочинав розробку стандарту 802.11i, покликаного усунути ці недоліки.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

Однак процес його створення затягнувся, в зв'язку з чим один з начерком (Draft 3) став використовуватися в якості проміжного рішення.

Цей стандарт отримав назву Wi-Fi Protected Access (WPA). В WPA для автентифікації станції і мережі може використовуватися інфраструктура 802.1 X або загальний ключ. На відміну від WEP ключі шифрування генеруються при встановленні з'єднання, а не розподіляються статично. Після успішної автентифікації сервер RADIUS передає станції значення, яке використовується для ідентифікації даної сесії – кельмою (МК). Станція і сервер RADIUS на основі МК виводять Pairwise Master Key (PMK), який передається точці доступу сервером RADIUS. Для генерації PMK використовується псевдовипадкова функція (PRF), заснована на хеш-функції HMAC-SHA-1. Отримане значення ключа прив'язується до поточної сесії між точкою доступу і станцією.

Ключ PMK потім використовується точкою доступу і клієнтом для генерації ключа Pairwise Transient Key (PTK). Ключ PTK, довжина якого складає 512 біт, надалі розділяється на 4 ключі: Key Confirmation Key (KCK), Key Encryption Key (KEK) і два ключі шифрування Temporal Key 1 і 2 (TK1 / TK2).

Ключ KCK застосовується в процесі виведення ключів шифрування для автентифікації клієнта. Значення KEK, використовується для захисту ключів шифрування широкомовного і групового трафіку Group Transient Key (GTK). Ключ GTK повинен бути однаковий для всіх станцій однієї мережі (BSS), тому він генерується точкою доступу і передається всім станціям. Ключі TK1 / TK2 застосовуються для захисту трафіку. Конкретні деталі їх застосування залежать від використовуваного криптоалгоритму.

Процес генерації ключа PMK заснований на обміні чотирма керуючими повідомленнями (4-way handshake, см IEEE802.11i):

- точка доступу відсилає станції випадкове число ANonce;
- станція генерує випадкове число SNonce і використовує функцію PRF-512 для виведення PTK на підставі PMK, ANonce, SNonce і MAC-адрес пристроїв. Значення SNonce відсилається на точку доступу, причому це повідомлення

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

захищається за допомогою функції контролю цілісності, що розраховується на основі ключа КСК;

- точка доступу отримує SNonce, виводить значення РТК і перевіряється цілісність повідомлення за допомогою отриманого значення КСК. Якщо дані коректні, станції відсилається інформація про підтримувані режими безпеки і ключ GTK;

- станція перевіряє параметри безпеки на збіг із значеннями, отриманими під час сканування (в Beacon або Probe Response), і цілісність отриманого повідомлення. Якщо відхилень не виявлено – точці доступу відсилається що підтверджує пакет.

В якості алгоритму шифрування в WPA використовується Temporary Key Integrity Protocol (TKIP), заснований на RC4, що дозволяє реалізувати сумісність з устаткуванням, що підтримує WEP. При використанні TKIP довжина вектора (TKIP Sequence Counter, TSK) ініціалізації збільшена до 48 байтів, що знижує ймовірність його повторення.

Ключ шифрування перемішується з MAC-адресою і TSK, і отримане значення використовується в якості ключа RC4. Таким чином, при застосуванні TKIP для кожного пакета використовується свій унікальний ключ WEP.

Таким чином, WPA вирішує такі проблеми WEP:

- статичний ключ шифрування;
- відсутність контролю цілісності повідомлень;
- недостатня довжина вектора ініціалізації.

Використання RC4 в якості основного алгоритму шифрування вже не задовольняє сучасним вимогам безпеки. У зв'язку з цим в стандарті 802.11i описується обов'язкове використання протоколу Counter Mode with CBC-MAC Protocol (CCMP) для шифрування трафіку.

У цьому протоколі, описаному в RFC 2610, використовується в якості криптографічного примітиву алгоритм AES-128, який є в цей час державним стандартом Сполучених Штатів Америки.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

У таблиці 1.3 наведено відповідність між різними назвами протоколів захисту бездротових мереж і криптоалгоритмами, які ними використовуються.

Таблиця 1.3

Стандарти захисту безпроводних мереж

Назва	Стандарт	Функції безпеки	Інші назви
WPA	802.11i, Draft 3	TKIP, RC4	Transition Security Network (TNS)
WPA2	802.11i	TKIP, RC4, CCMP, RC4, AES/RC4	Robust Security Network (RNS)

Як видно з таблиці, підтримка WPA2 або 802.11i означає, що для шифрування може використовуватися TKIP. В налаштуваннях підключення до бездротової мережі можна вибрати як WPA-TKIP, так і WPA2-TKIP.

Однак пристрої, які не підтримують WPA2 (наприклад, КПК на базі Windows Mobile), не можуть працювати з мережею, налаштовану на використання WPA2-TKIP, в зв'язку з деякими відмінностями в процесі встановлення з'єднання.

Висновки до першого розділу:

У першому розділі детально досліджено принципи побудови та функціонування технологій та протоколів, які використовуються для створення захищених локальних мереж. Розглянуто технології DHCP, SSH, WPA2-TKIP та інші. Визначено їхні переваги, недоліки та можливості застосування в корпоративних мережах. Зроблено висновок, що правильно налаштовані технології забезпечують високий рівень безпеки та надійності мережі.

РОЗДІЛ 2. ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ ЛОКАЛЬНОЇ МЕРЕЖІ

2.1. Проєктування фізичної топології мережі

Для проведення реконфігурації комп'ютерної мережі необхідно розуміти як саме мережеве обладнання пов'язане один з одним та в якій послідовності воно підключене, саме топологія комп'ютерної мережі дає змогу це зрозуміти. Однією з важливих характеристик комп'ютерної мережі є її топологія, яка характеризує усереднену геометричну схему розташування котрої входять до складу мережі комп'ютерів, вузлів комутації і каналів зв'язку. Сьогодні, коли географічні рамки мереж масштабуються, щоб з'єднати користувачів з різних міст і країн, системи перетворюються в глобальну обчислювальну мережу, а кількість комп'ютерів в мережі вже може варіюватися від десятка до декількох тисяч. При виборі топології локальної мережі враховується безліч критеріїв, як технічних, так і фінансових [4].

Зміни топології можуть відігравати важливу роль в процесі налаштуванні кожної функціональної області локальної мережі. У простій мережі з декількох комп'ютерів чітко видно, як з'єднані між собою різні компоненти. Чим більше розростається мережа, тим складніше стає відстежування місця розташування кожного компонента і його зв'язку з мережею. В дротовій мережі для підключення до всіх вузлів використовується безліч кабелів і мережевих пристроїв.

Схема допомагає зрозуміти, яким чином пристрої у великій мережі пов'язані між собою. При монтажі мережі складається схема фізичної топології, на якій вказано положення кожного вузла і спосіб його підключення до мережі. Крім того, там відзначені всі дроти і мережеві пристрої, що з'єднують хости. Така схема використовує символи або значки для представлення різних пристроїв і каналів, з яких складається мережа.

Топологія мережі вказує не тільки на фізичне розташування комп'ютерів, як часто вважають, але, і на характер зв'язків між ними, особливості поширення інформації, сигналів через мережу.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

Саме характер зв'язків визначає ступінь відмовостійкості і продуктивності мережі, необхідний рівень мережевої апаратури, найбільш придатний метод керування обміном, можливі типи середовищ передачі (каналів зв'язку), допустимий розмір мережі і багато іншого.

Розрізняють фізичну і логічну топологію. Логічна і фізична топології мережі незалежні один від одного. Фізична топологія – це геометрія побудови мережі, а логічна топологія визначає напрямки потоків даних між вузлами конкретної мережі і способи передачі даних між цими вузлами.

Спроектована мережа представлена на рисунку 2.1:

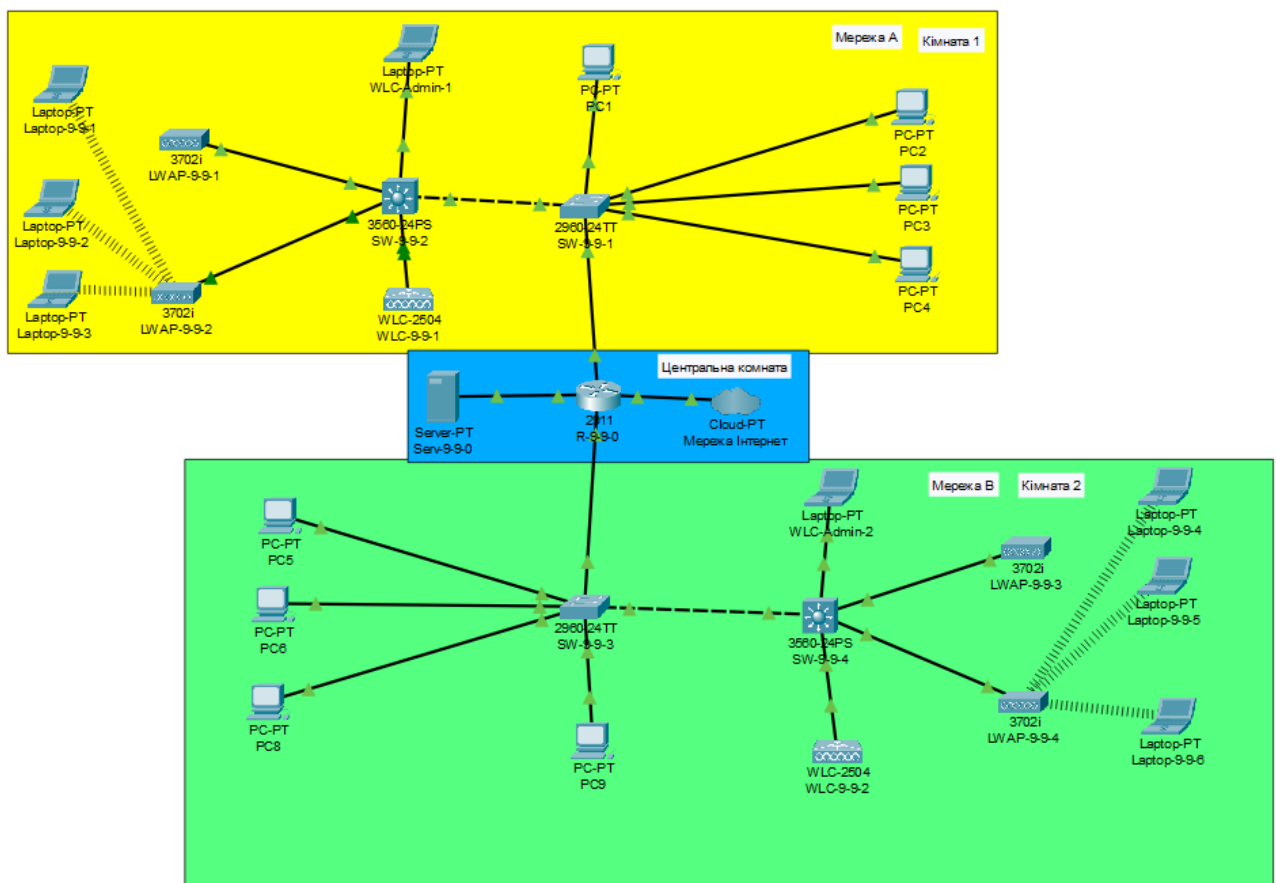


Рисунок. 2.1. – Проект фізичної топології мережі

Для забезпечення високої продуктивності роботи мережі використовуються лінії зв'язку Gigabit Ethernet. Кінцеві вузли під'єднанні до комутаційного обладнання за допомогою ліній зв'язку Fast Ethernet.

Присутня можливість розширення мережі.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

2.2. Проектування логічної (L3) топології мережі та розробка системи IP-адресації

Для функціонування мережі було виконано розрахунок параметрів IP-адресації. Під час розрахунку також було прийнято до уваги економію IP-адрес, тому мережі було розбито на підмережі з оптимальними масками, що відповідають кількості вузлів у кожній підмережі. Також було приділено увагу можливості розширення підмереж.

Для маршрутизаторів, комутаторів та серверів буде призначена динамічну IP-адресу, для робочих станцій IP-адресу видаватиме DHCP-сервер відповідної підмережі.

Далі у таблицях 2.1 – 2.2 наведений розрахунок IP-адрес для підмереж.

Таблиця 2.1

Адресація підмереж А

Призначення	IP-адреса
Адреса мережі	200.9.9.0 /24
Маска мережі	255.255.255.0
Інвертована маска	0.0.0.255
Мінімальна адреса	200.9.9.1
Максимальна адреса	200.9.9.254
Широкомовна адреса	200.9.9.255
Шлюз за замовчуванням	200.9.9.1
Діапазон адрес комутаторів	200.9.9.2 - 200.9.9.4
Діапазон адрес майбутніх ПК	200.9.9.5 - 200.9.9.254

Таблиця 2.2

Адресація підмереж В

Призначення	IP-адреса
Адреса мережі	201.9.9.0 /24

Адресація підмереж В

Призначення	ІР-адреса
Маска мережі	255.255.255.0
Інвертована маска	0.0.0.255
Мінімальна адреса	201.9.9.1
Максимальна адреса	201.9.9.254
Широкомовна адреса	201.9.9.255
Шлюз за замовчуванням	201.9.9.1
Діапазон адрес комутаторів	201.9.9.2 - 200.9.9.4
Діапазон адрес майбутніх ПК	201.9.9.5 - 200.9.9.254

2.3. Проектування служб та сервісів прикладного рівня

Протокол динамічного налаштування вузла версії 4 (DHCPv4, Dynamic Host Configuration Protocol v4) динамічно призначає IPv4-адреси та інші мережні параметри IPv4. Оскільки настільні ПК зазвичай складають основну частину мережних вузлів, DHCPv4 є надзвичайно корисним інструментом, що дозволяє мережним адміністраторам значно економити час.

У кожній підмережі є свій DHCP-сервер із встановленими діапазонами видаваних IP-адрес робочим станціям мережі. Роль DHCP-сервера виконуватиме маршрутизатор підмережі.

Протокол мережевого часу (Network Time Protocol, NTP) – це протокол, який допомагає синхронізувати час комп'ютерів у мережі. Цей протокол є прикладним протоколом, який відповідає за синхронізацію хостів у мережі TCP/IP.

У кожній підмережі знаходитиметься свій NTP-сервер, який служитиме еталонним джерелом часу та синхронізуватиме час з пристроями підмережі.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

Syslog – це стандартний протокол реєстрації повідомлень, який комп'ютерні системи використовують для надсилання журналів подій на сервер Syslog для зберігання. На мережевих пристроях Syslog може використовуватися для реєстрації таких подій, як зміна стану інтерфейсу, перезавантаження системи тощо. Можна реєструвати багато різних типів подій. Журнали мають важливе значення при усуненні несправностей, вивченні причин інцидентів і т.д.

Сервер Syslog дозволяє нам надсилати інформацію журналу всіх наших мережевих пристроїв в одне централізоване місце. Повідомлення журналу надсилаються через UDP-порт 514 на сервер Syslog. Звідси ми можемо шукати, керувати та архівувати всю інформацію журналу.

Широкий спектр пристроїв підтримує протокол Syslog, отже, він може бути використаний для реєстрації різних типів подій, таких як журнали з вебсервера, маршрутизатора і т.д.

2.4. Проектування підсистеми мережного захисту

На кожному маршрутизаторі та комутаторах підмереж будуть встановлені по 3 користувачі:

- Користувач Admin з найвищим рівнем доступу (15);
- Користувач Ingenger з середнім рівнем доступу (5);
- Користувач User з найнижчим рівнем доступу (1).

Створені паролі будуть 5 типу, тобто шифруватимуться за допомогою хешування MD5.

Також буде налаштовано віддалений доступ. Можливість підключення надаватиметься лише пристроям з однієї підмережі, підключення по SSH з пристроїв інших підмереж блокуватиметься.

Для входу в привілейований режим також необхідно буде ввести пароль, 5 типу шифрування.

Доступ до маршрутизаторів рівня ядра та розподілу буде можливий лише по прямому консольному підключенню та буде захищений паролем.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

В налаштуваннях підключення до бездротової мережі було вибрано WPA2-TKIP

2.5 Огляд основних загроз для комп'ютерної мережі

Для аналізу загроз у даній мережі, потрібно врахувати декілька аспектів: фізичну безпеку, мережеву безпеку, захист даних та відповідність вимогам. Розглянемо основні загрози, що можуть впливати на вашу мережу.

Фізичні загрози

- несанкціонований доступ до обладнання: Якщо фізичний доступ до маршрутизаторів, комутаторів та серверів не контролюється, зловмисники можуть втрутитися в налаштування або викрасти пристрої;
- стихійні лиха: Пожежі, повені та інші природні катастрофи можуть пошкодити мережеве обладнання.

Мережеві загрози

- атаки на мережевий рівень;
- ddos-атаки (Distributed Denial of Service): Зловмисники можуть перевантажити вашу мережу великим обсягом трафіку, що призведе до збоїв у роботі;
- сканування портів та вразливостей: Зловмисники можуть сканувати відкриті порти та вразливості у вашій мережі для подальших атак;
- незахищені протоколи: Використання незашифрованих протоколів, таких як Telnet або FTP, може призвести до перехоплення даних;
- атаки типу "Людина посередині" (Man-in-the-Middle): Зловмисники можуть перехопити або змінити трафік між вузлами мережі.

Загрози до даних

- перехоплення даних: Якщо дані передаються незашифрованими, зловмисники можуть їх перехопити;
- несанкціонований доступ до конфіденційних даних: Відсутність контролю доступу може призвести до несанкціонованого доступу до конфіденційної інформації.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

Програмні загрози

- шкідливе програмне забезпечення (Malware): Віруси, трояни та інше шкідливе ПЗ можуть вразити робочі станції, сервери та мережеві пристрої;
- вразливості в програмному забезпеченні: Використання застарілих або вразливих версій ОС та ПЗ може призвести до компрометації систем.

Атаки на рівні користувачів

- фішинг: Зловмисники можуть використовувати соціальну інженерію, щоб отримати конфіденційну інформацію від користувачів;
- атаки за допомогою соціальної інженерії: Маніпуляції користувачами для отримання доступу до мережевих ресурсів.

Неправильна конфігурація мережі

- відкриті порти та служби: Неправильно налаштовані порти або служби можуть стати точками входу для зловмисників;
- неправильні налаштування безпеки: Відсутність шифрування, неправильні ACL, відсутність моніторингу та журналювання можуть призвести до збоїв у безпеці.

Висновки до другого розділу:

У другому розділі проведено проектування фізичної топології мережі, розроблено систему IP-адресації, спроектовано підсистеми мережного захисту, такі як: доступ за користувачами та базовий захист, віддалений доступ та захист точок доступу Wi-Fi. Також у розділі розглянуто основні загрози для мережі, такі як шкідливе програмне забезпечення, фішинг, атаки за допомогою соціальної інженерії, неправильно налаштовані порти та служби.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

РОЗДІЛ 3. ВИБІР ОБЛАДНАННЯ, ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ ПРОЄКТОВАНОЇ ЛОКАЛЬНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

3.1. Вибір обладнання та ОС пристроїв для розробленого проєкту мережі

Для забезпечення функціонування даної мережі організації було обрано оптимальні маршрутизатори корпорації Cisco, котрі мають адаптованість під модернізацію модулями та підтримували технології Gigabit Ethernet.

Комутатори Cisco Catalyst 2960 серії є лінійкою комутаторів із фіксованою конфігурацією та портами Fast Ethernet і Gigabit Ethernet, що мають розширені LAN сервіси для підприємств початкового рівня та мереж віддаленого офісу. Комутатори Cisco Catalyst 2960 підтримують передачу голосу, даних і відео, а також безпечний доступ. Крім того, вони надають масштабоване управління в міру зміни потреб вашого бізнесу.

Комутатори Cisco Catalyst 2960 підтримують Intelligent features (створення складних списків управління доступом, розширена безпека), комбіновані гігабітні аплінки (мідний 10/100/1000BASE-T Ethernet або SFP-модуль для переходу в інше середовище – Cisco 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX, 100BASE-FX, 100BASE-LX, CWDM SFP). Також, пристрої Catalyst 2960 підтримують QoS, покроковий Rate Limiting, ACL (на базі MAC або IP-адрес, портів UDP/TCP) і multicast services, можливість регулювати швидкість передавання на кожному порту з кроком 64 кбіт, Link Aggregation для організації швидкісніших з'єднань між комутаторами і серверами, можливість організації транкових з'єднань на кожному порту за допомогою тегів 802.1q, до 255 VLAN на комутатор, до 4000 VLAN ID і управління через Cisco Network Assistant (підтримує широкий спектр моделей комутаторів від Cisco Catalyst 2960 до Cisco Catalyst 4506).

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

Прошивка комутаторів Cisco Catalyst 2960 випускається в образах LAN Base і Lan Lite Image. LAN Base має ширший функціонал, включно з поліпшеною безпекою (ACLs), DHCP Snooping і додатковими функціями з контролю доступу - Web authentication і розширення 802.1x, додатковими можливостями налаштувань якості обслуговування QoS, підтримкою надлишкового живлення RPS і великої кількості SFP-портів. Функції Flex Links і Link State Tracking, збільшена кількість підтримуваних VLANs (до 256), IPv6 Host, MLD Snooping, LLDP-MED, RSPAN, MVR, DHCP Option 82, IP SLA (responder) та інше.



Рисунок 3.1 – Комутатори Cisco Catalyst 2960

Маршрутизатори Cisco серії 2900 базуються на кращих у своєму класі характеристиках наявних маршрутизаторів Cisco серії 2800 і представлені чотирма платформами (рис. 1): маршрутизатори Cisco 2901, 2911, 2921 і 2951 з інтегрованими послугами.

Всі маршрутизатори Cisco серії 2900 мають вбудоване апаратне прискорення шифрування, слоти для цифрових сигнальних процесорів (DSP) з підтримкою передачі голосу та відео, додатковий міжмережевий екран, засоби захисту від вторгнень, обробки викликів, голосової пошти та додатків. Крім того, платформи підтримують найширший в галузі спектр дротових і бездротових варіантів підключення, таких як T1/E1, T3/E3, xDSL, мідний і оптоволоконний GE.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		46



Рисунок 3.2 – Маршрутизатор Cisco 2911

Серія Cisco 2900 розроблена для задоволення вимог сучасних філій з можливістю гнучкого проєктування для майбутніх додатків. Модульна архітектура розроблена для підтримки зростаючих вимог до пропускної здатності, з'єднань з мультиплексуванням з часовим поділом каналів (TDM) і повністю інтегрованого розподілу живлення між модулями з підтримкою стандартів 802.3af Power over Ethernet (PoE) і Cisco Enhanced PoE (ePoE).

Серія Cisco 2900 забезпечує значно розширені модульні можливості пропонуючи захист інвестицій для клієнтів. Більшість модулів, доступних на попередніх поколіннях маршрутизаторів Cisco, таких як Cisco 2800 Series, підтримуються на маршрутизаторах Cisco 2900 Series. Крім того, модулі можуть використовуватися на інших підтримуваних платформах Cisco для забезпечення максимального захисту інвестицій. Використання загальних інтерфейсних карт в мережі значно знижує складність управління вимогами до інвентаризації, реалізації великих розгортань мережі та підтримки конфігурацій в різних за розміром філіях.

Маршрутизатори з інтегрованими послугами Cisco серії 2900 реалізують інноваційні технології під управлінням провідного в галузі програмного забезпечення Cisco IOS. Розроблені для широкого розгортання в найбільш вимогливих корпоративних мережах, мережах доступу і мережах провайдерів

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

послуг, платформи маршрутизаторів інтегрованих послуг покоління 2 підтримуються програмним забезпеченням Cisco IOS версій 15M&T.

Випуск 15.0(1)M доступний негайно і забезпечує підтримку повного портфеля технологій Cisco, включаючи функціональність і можливості, надані в релізах 12.4 і 12.4T. Нововведення в 15.0(1)M охоплюють кілька технологічних областей, включаючи безпеку, голос, високу доступність, IP-маршрутизацію і багатоадресну розсилку, якість обслуговування (QoS), IP-мобільність, багатопроTOCOLьну комутацію по мітках (MPLS), VPN і вбудоване управління.

Бездротовий контролер Cisco® серії 2500 забезпечує бездротові функції в системі в малих і середніх підприємствах і філіях. Розроблені для продуктивності 802.11n і 802.11ac, бездротові контролери Cisco серії 2500 є контролерами початкового рівня, які забезпечують зв'язок у реальному часі між точками доступу Cisco Aironet®, щоб спростити розгортання та роботу бездротових мереж (рис. 3.3).



Рисунок 3.3 – Бездротовий контролер Cisco® серії 2500

Будучи компонентом уніфікованої бездротової мережі Cisco, цей контролер забезпечує централізовані політики безпеки, можливості системи запобігання бездротовому вторгненню (wIPS), відзначене нагородами управління радіочастотами та якість обслуговування (QoS) для голосу та відео. Забезпечуючи продуктивність 802.11ac і масштабованість, Cisco серії 2500 забезпечує низьку загальну вартість володіння та гнучкість для масштабування в міру зростання вимог до мережі.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

Бездротовий контролер Cisco 2504 підтримує технологію Cisco Application Visibility and Control (AVC), яка включає систему розпізнавання програм на основі мережі Cisco 2 (NBAR-2). N-BAR-2 здійснює глибоку перевірку пакетів (DPI) для класифікації додатків і зв'язування з якістю обслуговування (QoS), щоб або відкинути, або позначити трафік, таким чином віддаючи пріоритет критично важливим для бізнесу додаткам у мережі. Cisco AVC використовує NetFlow версії 9 для експорту потоків до інфраструктури Cisco Prime™ або стороннього NetFlow Collector. Бездротовий контролер Cisco 2504 також підтримує каталог послуг Bonjour, що дозволяє рекламувати та використовувати служби Bonjour (Apple) в окремій мережі рівня 3. Механізм політики бездротового зв'язку – це функція профілювання бездротового зв'язку та політики бездротового контролера Cisco серії 2500, яка дає змогу профілювати бездротові пристрої та застосовувати такі політики, як призначення VLAN, QoS, ACL і доступ на основі часу доби.

Ліцензування точок доступу на основі бездротового контролера серії Cisco 2500 забезпечує гнучкість із 5, 15, 25 або 50 точками доступу. Додаткову підтримку точок доступу можна додати з кроком 1, 5 або 25.

3.2. Побудова та налагодження спроектованої локальної мережі

Перейдемо до створення та налаштування спроектованої мережі. Налаштування починається зі зміни стандартних імен елементів мережі та призначення визначених раніше IP-адрес. Приклад налаштування представлено на рисунку.

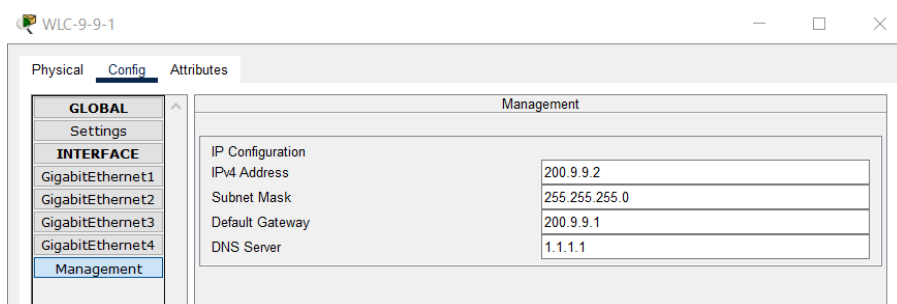


Рисунок 3.4 – Налаштування IP-адресації на WLC-9-9-1

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

```

R-9-9-0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-9-9-0(config)#in g0/0
R-9-9-0(config-if)#ip addr 200.9.9.1 255.255.255.0
R-9-9-0(config-if)#no shut
R-9-9-0(config-if)#exit
R-9-9-0(config)#ip dhcp pool R_1
R-9-9-0(dhcp-config)#network 200.9.9.0 255.255.255.0
R-9-9-0(dhcp-config)#default-router 200.9.9.1
R-9-9-0(dhcp-config)#dns-server 1.1.1.1
R-9-9-0(dhcp-config)#exit
R-9-9-0(config)#ip dhcp excluded-address 200.9.9.1 200.9.9.2
R-9-9-0(config)#in g0/1
R-9-9-0(config-if)#ip addr 201.9.9.1 255.255.255.0
R-9-9-0(config-if)#no shut
R-9-9-0(config-if)#exit
R-9-9-0(config)#ip dhcp pool R_2
R-9-9-0(dhcp-config)#network 201.9.9.0 255.255.255.0
R-9-9-0(dhcp-config)#default-router 201.9.9.1
R-9-9-0(dhcp-config)#dns-server 2.2.2.2
R-9-9-0(dhcp-config)#exit
R-9-9-0(config)#ip dhcp excluded-address 201.9.9.1 201.9.9.2
R-9-9-0(config)#end
R-9-9-0#
%SYS-5-CONFIG_I: Configured from console by console

R-9-9-0#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R-9-9-0#

```

Рисунок 3.5 – Налаштування IP-адресації на маршрутизаторі R-9-9-0

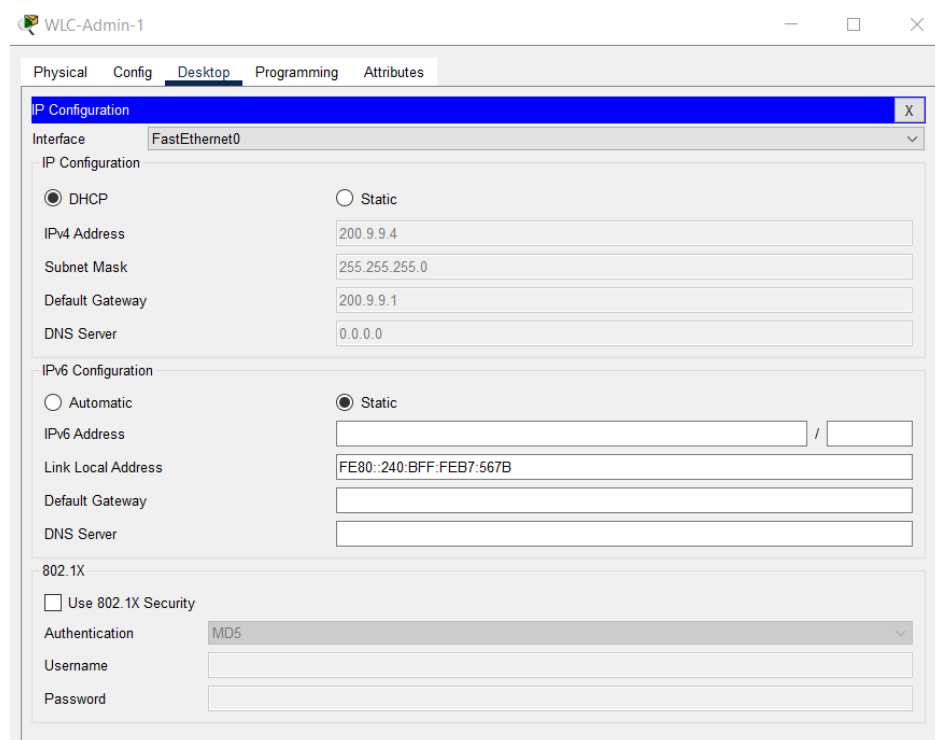


Рисунок 3.6 – Налаштування IP-адресації на WLC-Admin

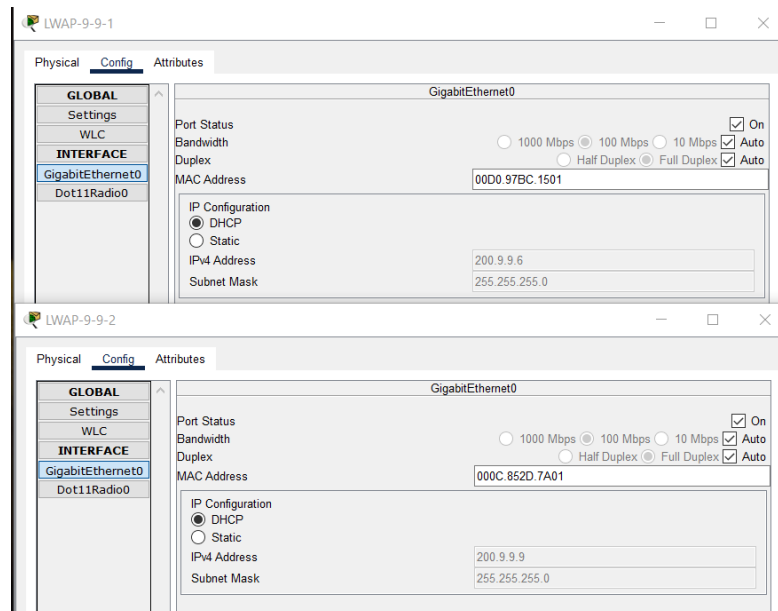


Рисунок 3.7 – Налаштування IP-адресації на LWAP-9-9-1 і LWAP-9-9-2

У побудованій мережі налагодити функціонування WLC на основі групування портів. Виконати додаткові налаштування, які забезпечать підвищення рівня захищеності побудованої мережі.

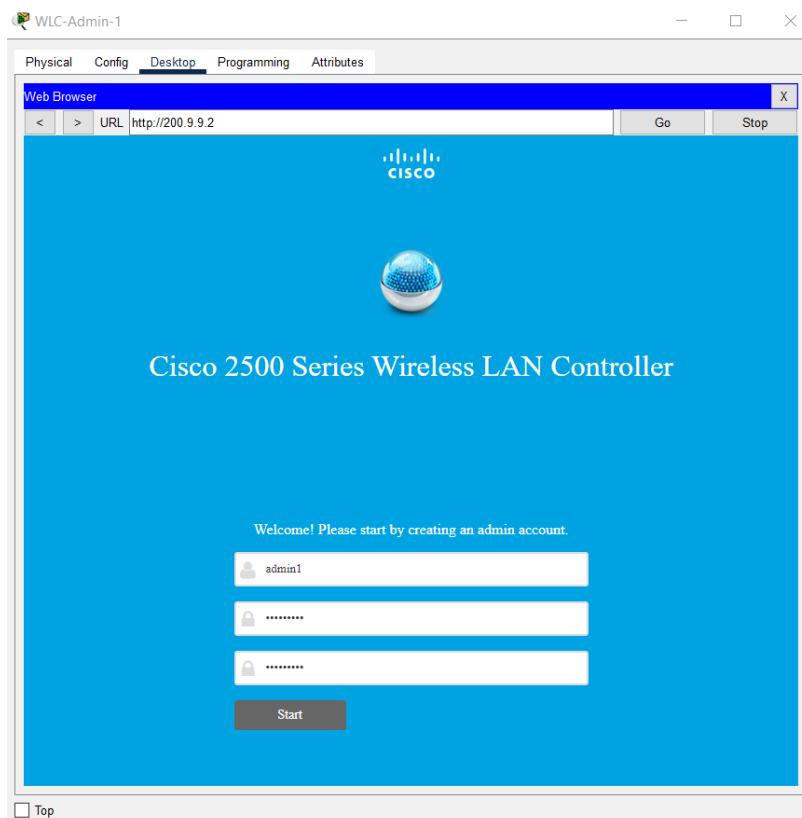


Рисунок 3.8 – Початкове налаштування WLC-9-9-1

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

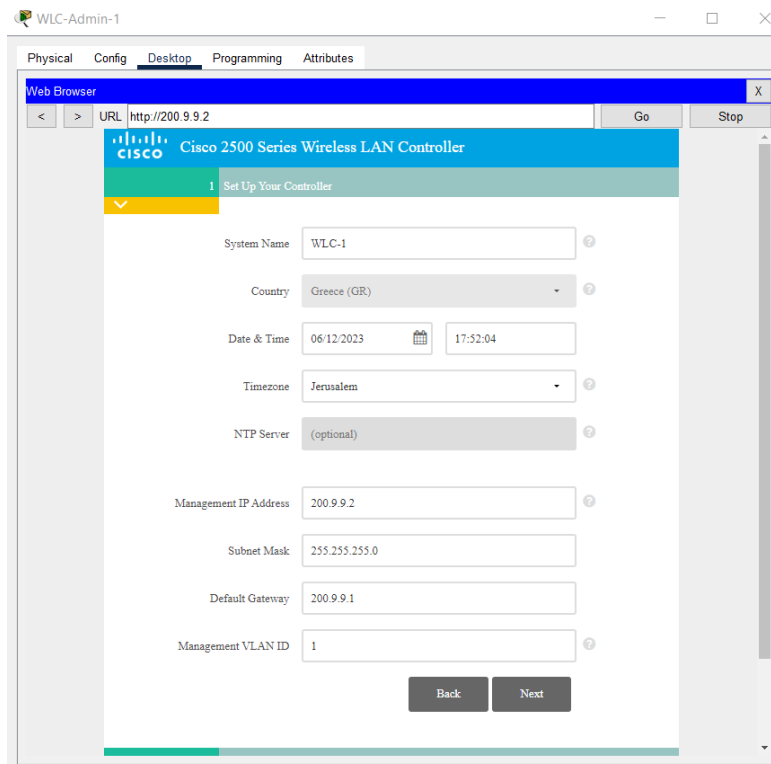


Рисунок 3.9 – Налаштування контролера на WLC-9-9-1

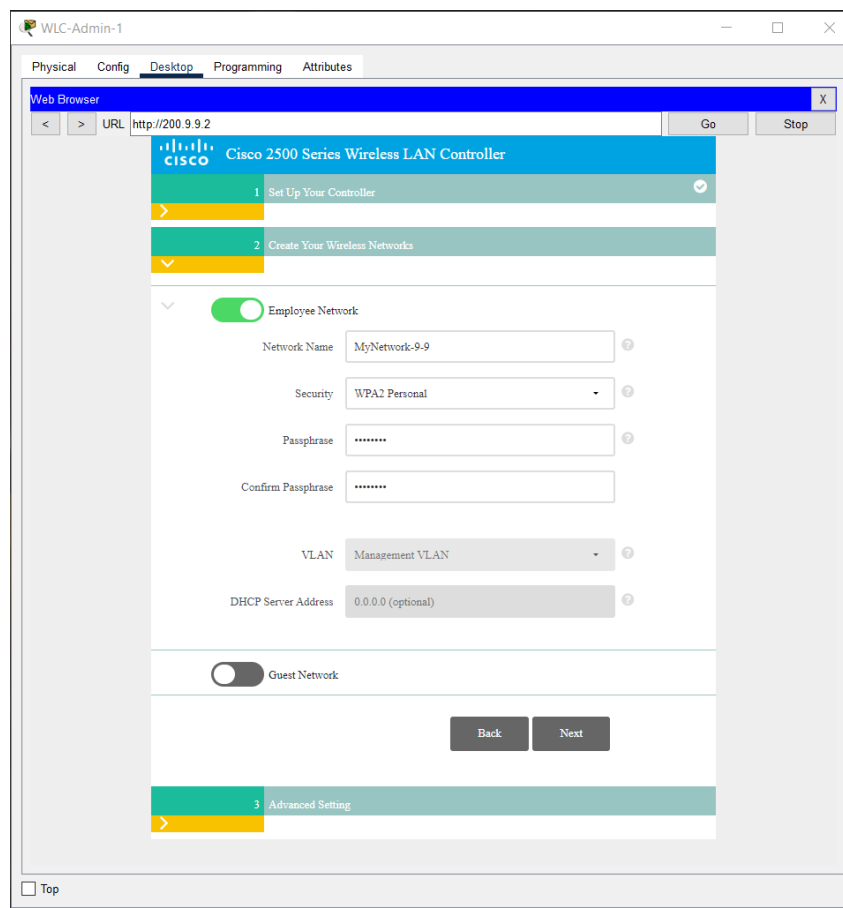


Рисунок 3.10 – Налаштування мережі на WLC-9-9-1

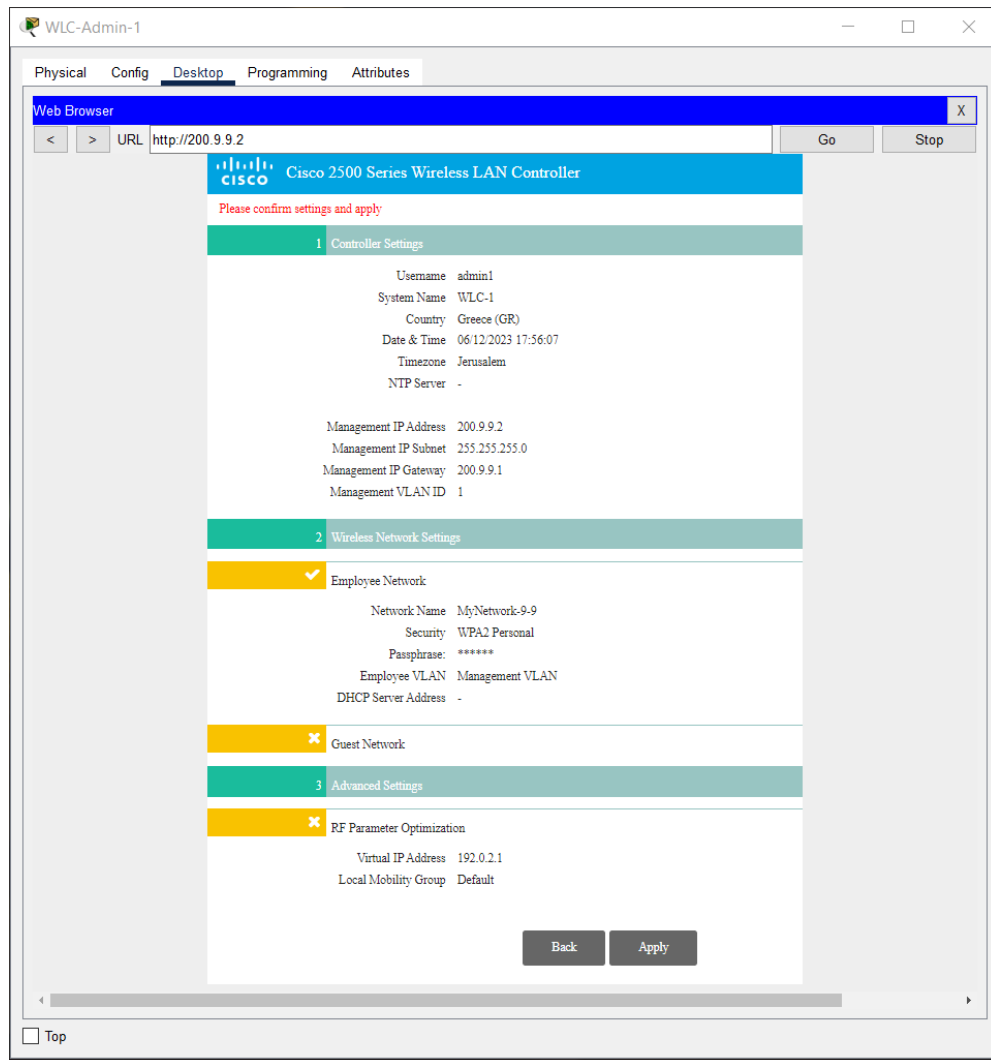


Рисунок 3.11 – Підсумок налаштувань на WLC-9-9-1

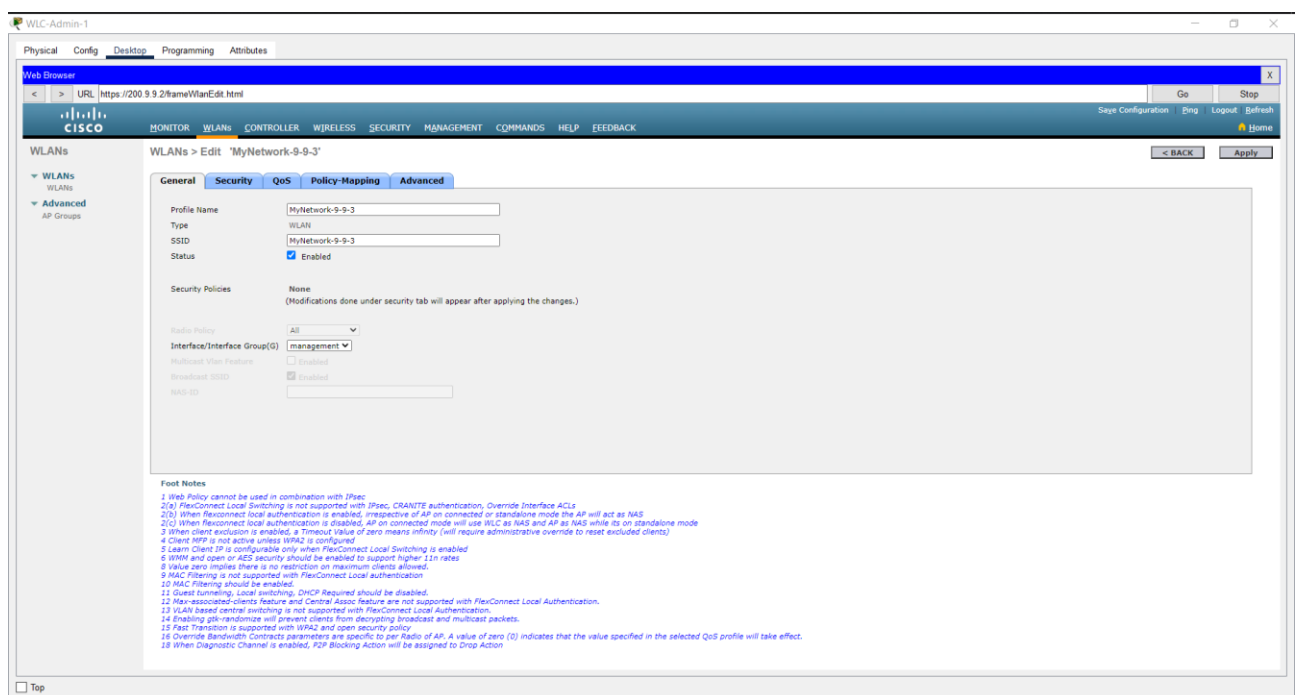


Рисунок 3.12 – Додавання другої VLAN налаштувань на WLC-9-9-1

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

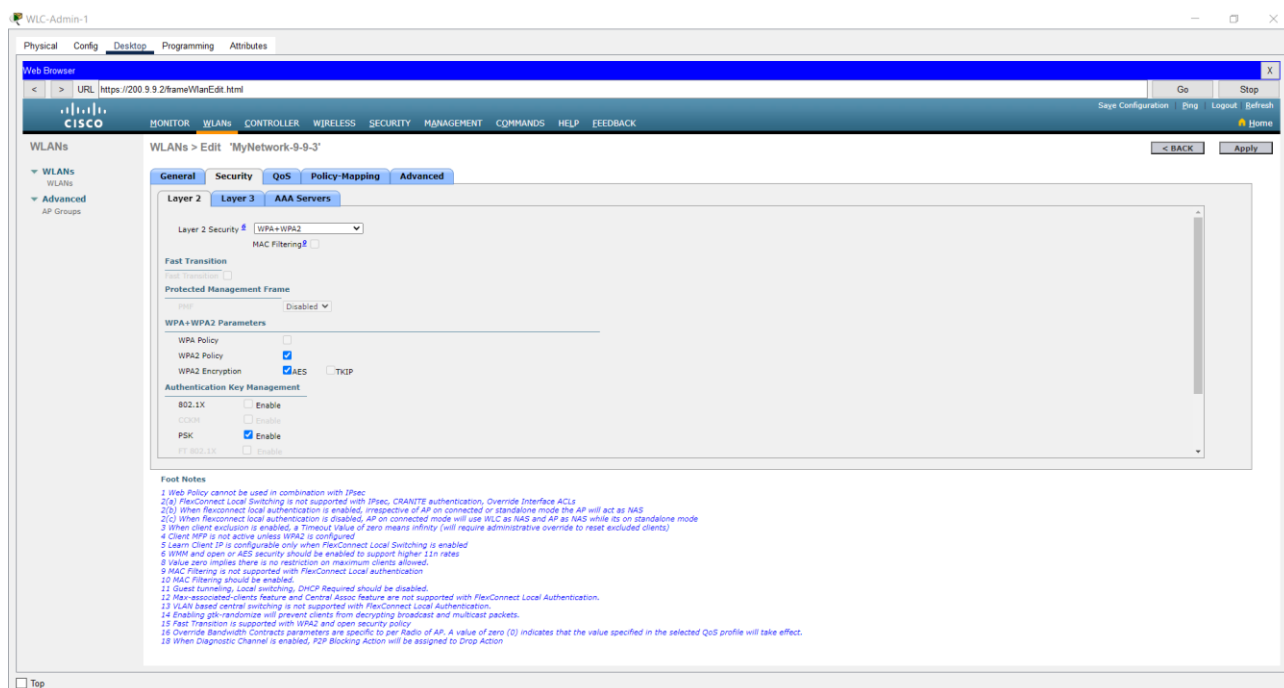


Рисунок 3.13 – Налаштувань захисту другої VLAN на WLC-9-9-1

Налагодити можливість LightWeight Access Point.

LightWeight Access Point (LWAP) – це тип точки доступу, яка працює під керуванням централізованого контролера бездротової мережі. Вона призначена для спрощення управління великою кількістю точок доступу.

AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	PoE Status	Sp Et
LWAP-9-9-2	200.9.9.9	AIR-CT5502-K9	00:0C:85:2D:7A:01	0 d, 1 h 3 m 40 s	Enabled	REG	-	10
LWAP-9-9-1	200.9.9.6	AIR-CT5502-K9	00:0D:97:BC:15:01	0 d, 1 h 3 m 48 s	Enabled	REG	-	10

Рисунок 3.14 – Перегляд успішно зареєстрованих точок доступу

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

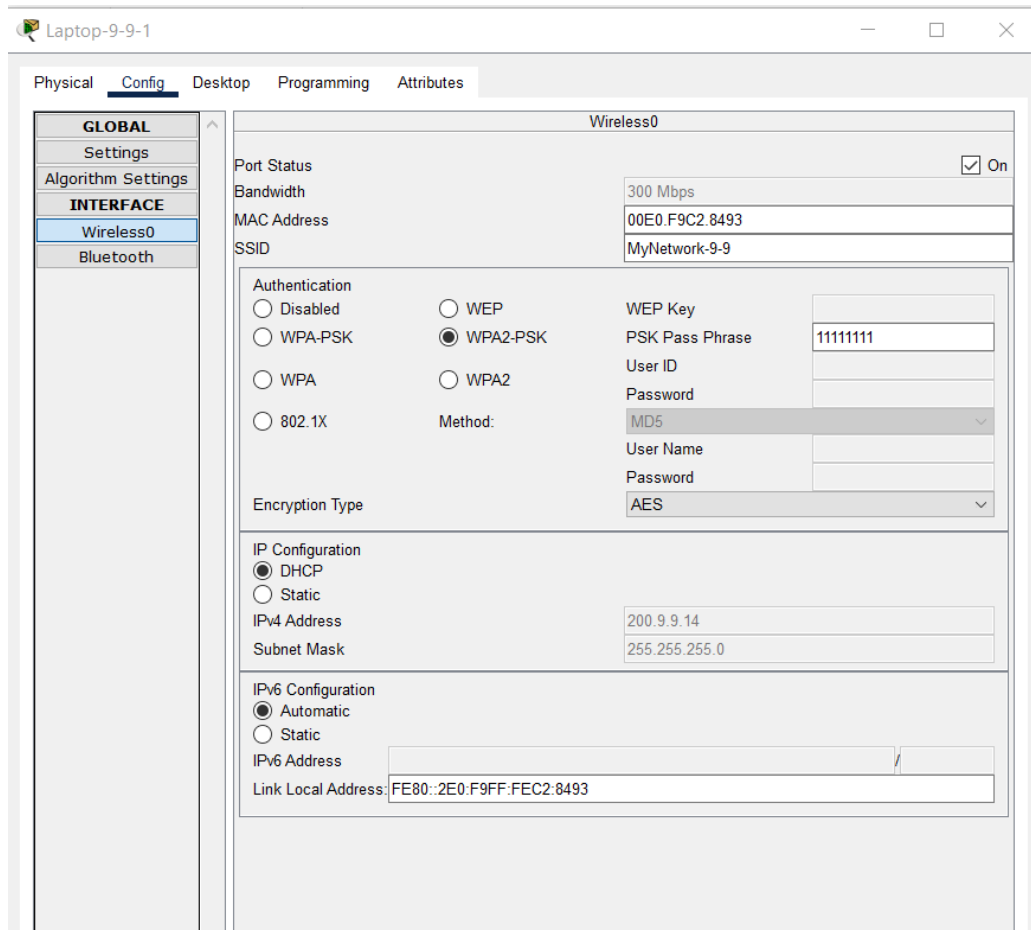


Рисунок 3.15 – Підключення до точки доступу та отримання IP-адреси на робочій станції Laptop-9-9-1

На другій частині мережі налаштування аналогічні, різниця лише в IP-адресації

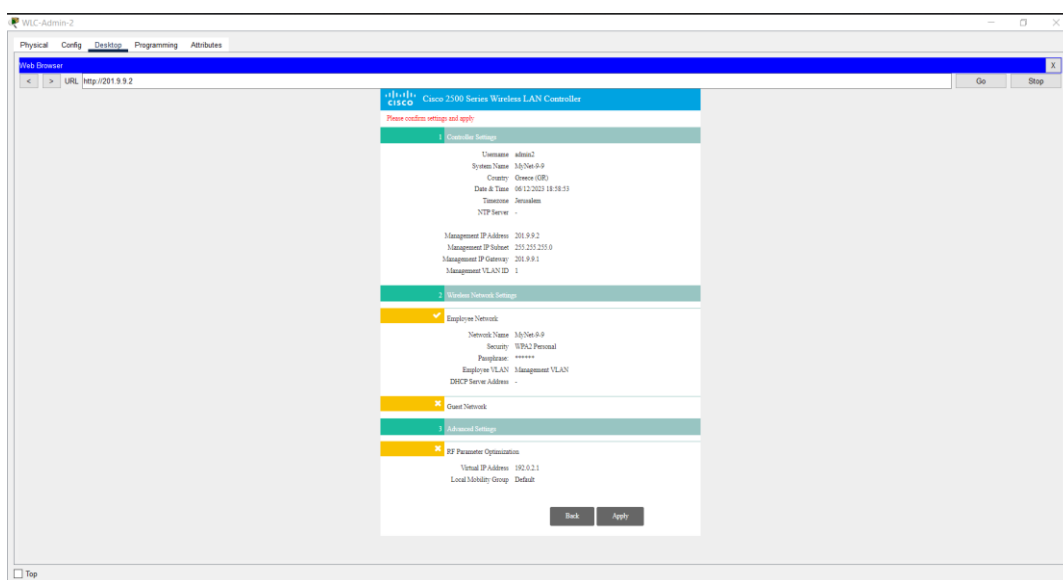


Рисунок 3.16 – Підсумок налаштувань на WLC-9-9-2

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

Тепер налагодимо засоби захисту та віддалений доступ. Створимо по 3 користувача з різними рівнями доступу, налаштуємо підключення по SSHv2, та налаштуємо пароль для входу в привілейований режим.

```
R-9-9-0>en
R-9-9-0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-9-9-0(config)#ip domain-name my.net
R-9-9-0(config)#username adminR0 privilege 15 secret admin
R-9-9-0(config)#username ingenerR0 privilege 5 secret ingener
R-9-9-0(config)#username userR0 privilege 1 secret user
R-9-9-0(config)#enable secret enable
R-9-9-0(config)#crypto key generate rsa
The name for the keys will be: R-9-9-0.my.net
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

R-9-9-0(config)#line vty 0 4
*Mar 1 0:21:35.546: %SSH-5-ENABLED: SSH 1.99 has been enabled
R-9-9-0(config-line)#login local
R-9-9-0(config-line)#transport input ssh
R-9-9-0(config-line)#transport output ssh
R-9-9-0(config-line)#end
R-9-9-0#
%SYS-5-CONFIG_I: Configured from console by console

R-9-9-0#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R-9-9-0#
```

Рисунок 3.17 – Налагодження засобів захисту та віддаленого доступу на прикладі маршрутизаторі R-9-9-0

```
SW-9-9-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-9-9-1(config)#ip domain-name my.net
SW-9-9-1(config)#username adminSW1 privilege 15 secret admin
SW-9-9-1(config)#username ingenerSW1 privilege 5 secret ingener
SW-9-9-1(config)#username userSW1 privilege 1 secret user
SW-9-9-1(config)#enable secret enable
SW-9-9-1(config)#crypto key generate rsa
The name for the keys will be: SW-9-9-1.my.net
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

SW-9-9-1(config)#line vty 0 4
*Mar 1 0:39:48.414: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW-9-9-1(config-line)#login local
SW-9-9-1(config-line)#transport input ssh
SW-9-9-1(config-line)#transport output ssh
SW-9-9-1(config-line)#end
SW-9-9-1#
```

Рисунок 3.18 – Налагодження засобів захисту та віддаленого доступу на прикладі комутатора SW-9-9-1

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

Налагодження засобів захисту та віддаленого доступу на інших комутаторах аналогічні

Налагодимо протокол маршрутизації EIGRP

```
R-9-9-0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-9-9-0(config)#router eigrp 1
R-9-9-0(config-router)#network 200.9.9.0
R-9-9-0(config-router)#network 201.9.9.0
R-9-9-0(config-router)#network 202.9.9.0
R-9-9-0(config-router)#exit
R-9-9-0(config)#exit
R-9-9-0#
```

Рисунок 3.19 – Налаштування EIGRP на маршрутизаторі R-9-9-0

Налагодимо протокол мережного часу NTP

Налаштування протоколу мережевого часу (NTP) дає такі можливості:

1. Синхронізація часу: Забезпечує точну синхронізацію часу між всіма пристроями в мережі.
2. Єдиний часовий стандарт: Усі пристрої використовують однаковий часовий стандарт, що спрощує управління мережею.
3. Безпека: Підвищує безпеку мережі за рахунок коректної роботи протоколів безпеки, що залежать від часу.

```
R-9-9-0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-9-9-0(config)#service timestamps log datetime msec
R-9-9-0(config)#service timestamps debug datetime msec
R-9-9-0(config)#clock timezone EEST 2
R-9-9-0(config)#end
R-9-9-0#
*Jun 23, 19:55:01.5555: SYS-5-CONFIG_I: Configured from console by console
R-9-9-0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-9-9-0(config)#ntp authentication-key 1111 md5 1111
R-9-9-0(config)#ntp trusted-key 1111
R-9-9-0(config)#ntp server 202.9.9.2 key 1111
R-9-9-0(config)#ntp update-calendar
R-9-9-0(config)#exit
R-9-9-0#
*Jun 23, 19:57:30.5757: SYS-5-CONFIG_I: Configured from console by console
R-9-9-0#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R-9-9-0#show ntp status
Clock is synchronized, stratum 2, reference is 202.9.9.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E8179936.000000259 (19:57:42.601 UTC Fri Jun 23 2023)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 44.86 msec, peer dispersion is 0.12 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system poll
interval is 4, last update was 6 sec ago.
R-9-9-0#
```

Рисунок 3.20 – Налаштування NTP на маршрутизаторі R-9-9-0

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

```

SW-9-9-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-9-9-2(config)#service timestamps log datetime msec
SW-9-9-2(config)#service timestamps debug datetime msec
SW-9-9-2(config)#clock timezone EEST 2
SW-9-9-2(config)#end
SW-9-9-2#
*Mar 01, 00:54:38.5454: SYS-5-CONFIG_I: Configured from console by console
SW-9-9-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-9-9-2(config)#ntp authentication-key 1111 md5 1111
SW-9-9-2(config)#ntp trusted-key 1111
SW-9-9-2(config)#ntp server 202.9.9.2 key 1111
SW-9-9-2(config)#ntp update-calendar
SW-9-9-2(config)#exit
SW-9-9-2#

SW-9-9-2#show ntp stat
Clock is synchronized, stratum 2, reference is 202.9.9.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E817970C.00000005E (19:48:28.094 UTC Fri Jun 23 2023)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 16.27 msec, peer dispersion is 0.11 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system poll
interval is 4, last update was 2 sec ago.
SW-9-9-2#

```

Рисунок 3.21 – Налаштування NTP на маршрутизаторі SW-9-9-2

Налагодження протоколу мережного часу NTP на інших комутаторах аналогічні

Налагодимо протокол NAT

```

R-9-9-0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-9-9-0(config)#access-list 1 permit 200.9.9.0 0.0.0.255
R-9-9-0(config)#access-list 1 permit 201.9.9.0 0.0.0.255
R-9-9-0(config)#access-list 1 permit 202.9.9.0 0.0.0.255
R-9-9-0(config)#
R-9-9-0(config)#in gi0/0
R-9-9-0(config-if)#ip nat outside
R-9-9-0(config-if)#exit
R-9-9-0(config)#in gi0/1
R-9-9-0(config-if)#ip nat inside
R-9-9-0(config-if)#exit
R-9-9-0(config)#in gi0/2
R-9-9-0(config-if)#ip nat inside
R-9-9-0(config-if)#exit
R-9-9-0(config)#ip nat inside source list 1 interface gigabitEthernet 0/0 overload
R-9-9-0(config)#end
R-9-9-0#
*Jun 23, 21:00:46.000: SYS-5-CONFIG_I: Configured from console by console
R-9-9-0#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R-9-9-0#

```

Рисунок 3.22 – Налаштування NAT та перевірка роботи протоколу на маршрутизаторі R-9-9-0

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

Налагодимо протокол SYSLOG

```
R-9-9-0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-9-9-0(config)#logging on
R-9-9-0(config)#logging 202.9.9.2
R-9-9-0(config)#logging trap informational
^
% Invalid input detected at '^' marker.

R-9-9-0(config)#logging trap info
^
% Invalid input detected at '^' marker.

R-9-9-0(config)#logging trap userinfo
^
% Invalid input detected at '^' marker.

R-9-9-0(config)#logging informational
^
% Invalid input detected at '^' marker.

R-9-9-0(config)#logging userinfo
R-9-9-0(config)#logging origin-id hostname
^
% Invalid input detected at '^' marker.

R-9-9-0(config)#logging trap informational
^
% Invalid input detected at '^' marker.

R-9-9-0(config)#logging buffered
R-9-9-0(config)#logging rate-limit
^
% Invalid input detected at '^' marker.

R-9-9-0(config)#exit
R-9-9-0#
*Jun 23, 20:38:12.3838: SYS-5-CONFIG_I: Configured from console by console
*Jun 23, 20:38:12.3838: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 202.9.9.2 port 514 started -
CLI initiated
```

Рисунок 3.23 – Налаштування протоколу Syslog на маршрутизаторі R-9-9-1

```
SW-9-9-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-9-9-2(config)#logging on
SW-9-9-2(config)#logging 202.9.9.2
SW-9-9-2(config)#logging userinfo
SW-9-9-2(config)#logging origin-id hostname
^
% Invalid input detected at '^' marker.

SW-9-9-2(config)#logging buffered
SW-9-9-2(config)#logging rate-limit
^
% Invalid input detected at '^' marker.

SW-9-9-2(config)#logging trap informational
^
% Invalid input detected at '^' marker.

SW-9-9-2(config)#exit
SW-9-9-2#
*Jun 23, 20:42:04.4242: SYS-5-CONFIG_I: Configured from console by console
*Jun 23, 20:42:04.4242: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 202.9.9.2 port 514 started -
CLI initiated
SW-9-9-2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
SW-9-9-2#
```

Рисунок 3.24 – Налаштування протоколу Syslog

Налагодження протоколу Syslog на інших комутаторах аналогічні

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

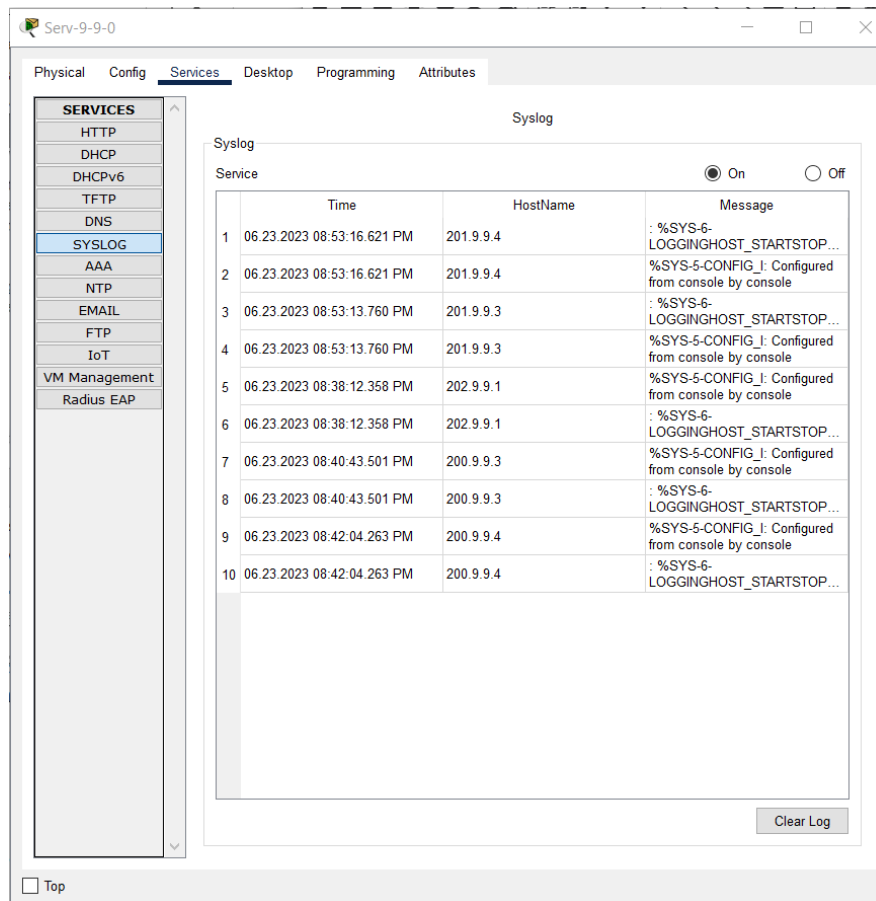


Рисунок 3.25 – Перевірка роботи протоколу Syslog

3.3. Тестування роботи створеної локальної мережі

Для початку перевіримо чи коректно працює DHCP-сервер:

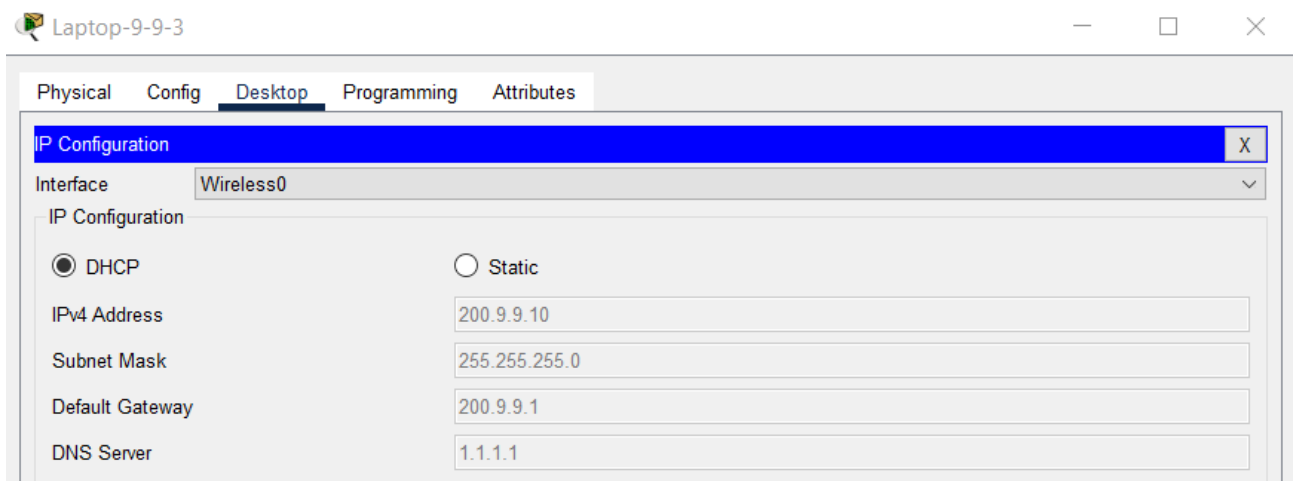


Рисунок 3.26 – Перевірка роботи DHCP на робочій станції Laptop-9-9-3

Для перевірки зв'язку між кінцевими пристроями, а також шляху пакета при передачі, використано команди ping та tracert.

Для початку перевірка зв'язку між пристроями локальної мережі, що підключені до одного маршрутизатора.

```

Laptop-9-9-2
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 200.9.9.10

Pinging 200.9.9.10 with 32 bytes of data:

Reply from 200.9.9.10: bytes=32 time=41ms TTL=128
Reply from 200.9.9.10: bytes=32 time=42ms TTL=128
Reply from 200.9.9.10: bytes=32 time=12ms TTL=128
Reply from 200.9.9.10: bytes=32 time=19ms TTL=128
Reply from 200.9.9.10: bytes=32 time=23ms TTL=128
Reply from 200.9.9.10: bytes=32 time=31ms TTL=128

Ping statistics for 200.9.9.10:
    Packets: Sent = 3, Received = 6, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 42ms, Average = 28ms

Control-C
^C
C:\>ping 200.9.9.14

Pinging 200.9.9.14 with 32 bytes of data:

Reply from 200.9.9.14: bytes=32 time=83ms TTL=128
Reply from 200.9.9.14: bytes=32 time=84ms TTL=128
Reply from 200.9.9.14: bytes=32 time=94ms TTL=128
Reply from 200.9.9.14: bytes=32 time=104ms TTL=128

Ping statistics for 200.9.9.14:
    Packets: Sent = 1, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 83ms, Maximum = 104ms, Average = 91ms

Control-C
^C
C:\>ping 200.9.9.8

Pinging 200.9.9.8 with 32 bytes of data:

Reply from 200.9.9.8: bytes=32 time=55ms TTL=128
Reply from 200.9.9.8: bytes=32 time=60ms TTL=128

Ping statistics for 200.9.9.8:
    Packets: Sent = 1, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 55ms, Maximum = 60ms, Average = 57ms

Control-C
^C
C:\>ping 200.9.9.1

Pinging 200.9.9.1 with 32 bytes of data:

Reply from 200.9.9.1: bytes=32 time=23ms TTL=255
Reply from 200.9.9.1: bytes=32 time=25ms TTL=255
  
```

Рисунок 3.27 – Перевірка зв'язку між робочими станціями підмережі А

Перейдемо до перевірки налаштованих засобів захисту та віддаленого доступу.

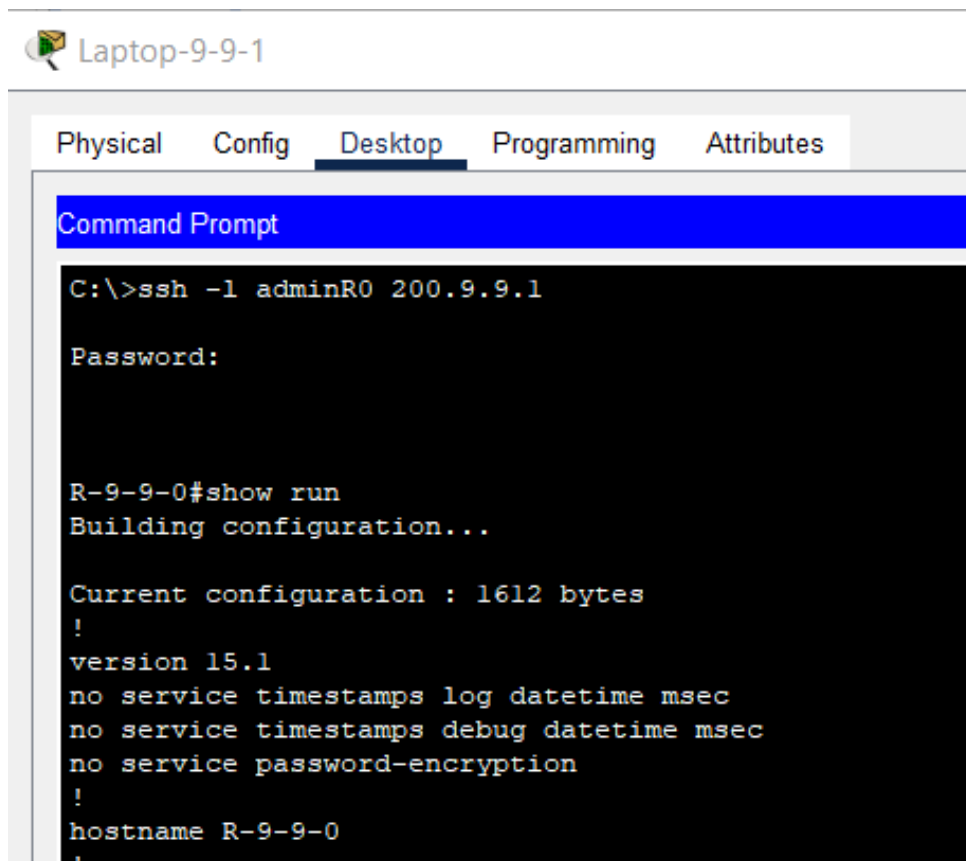


Рисунок 3.28 – Перевірка можливості підключення по SSH до пристрою цієї ж мережі

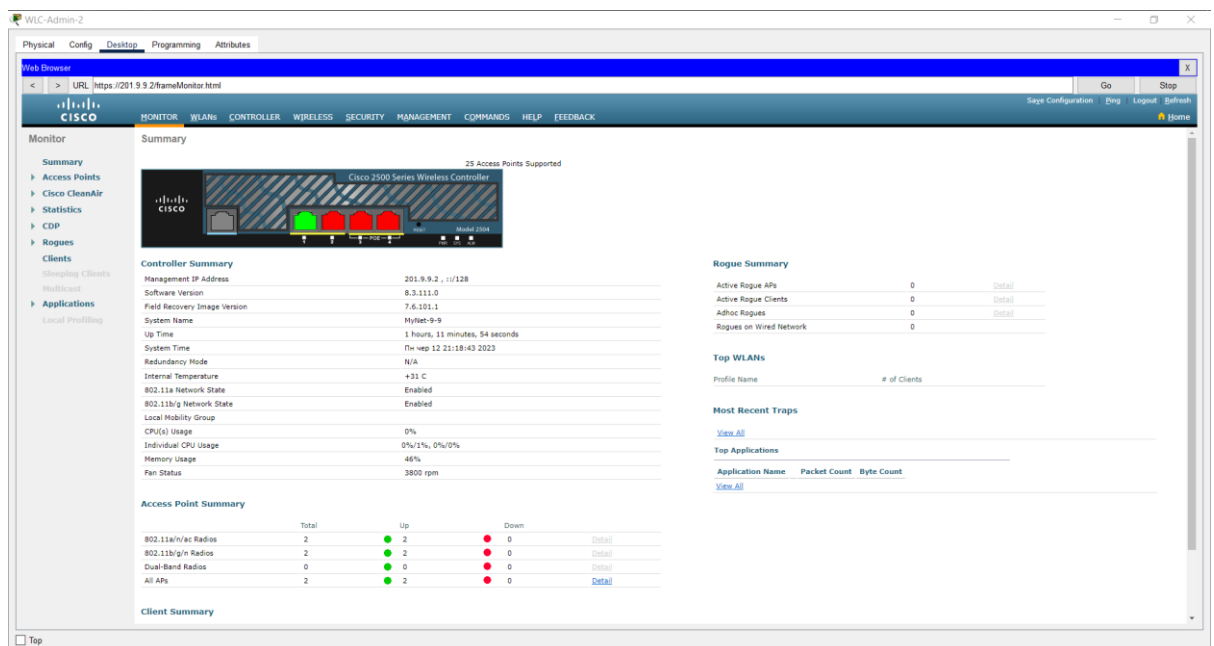


Рисунок 3.29 – Перегляд загальної інформації про роботу WLC

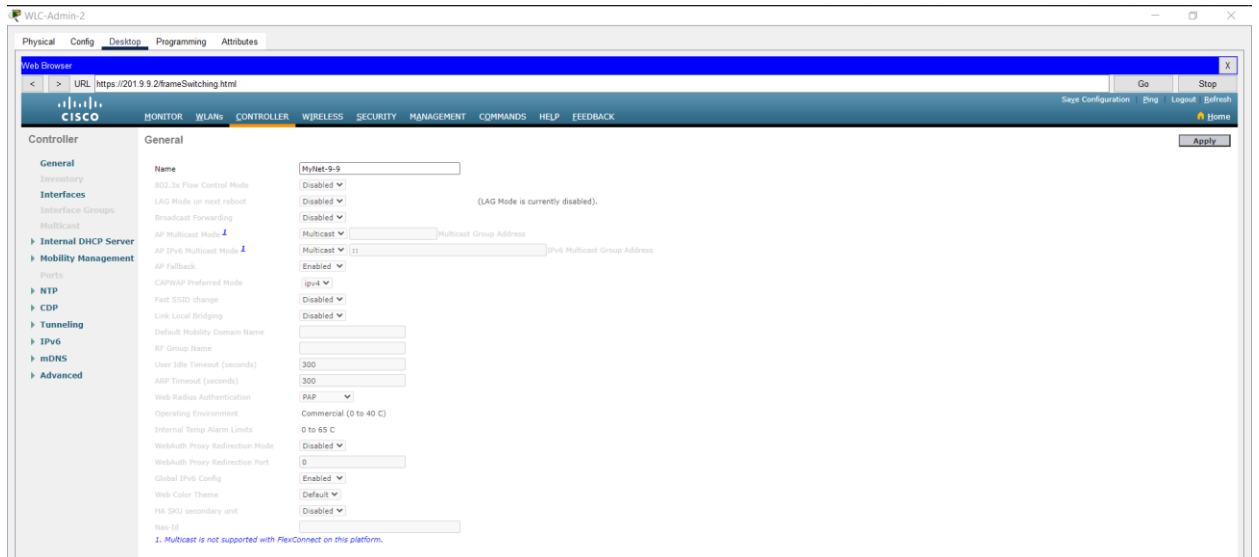


Рисунок 3.30 – Перегляд інформації про контролер WLC

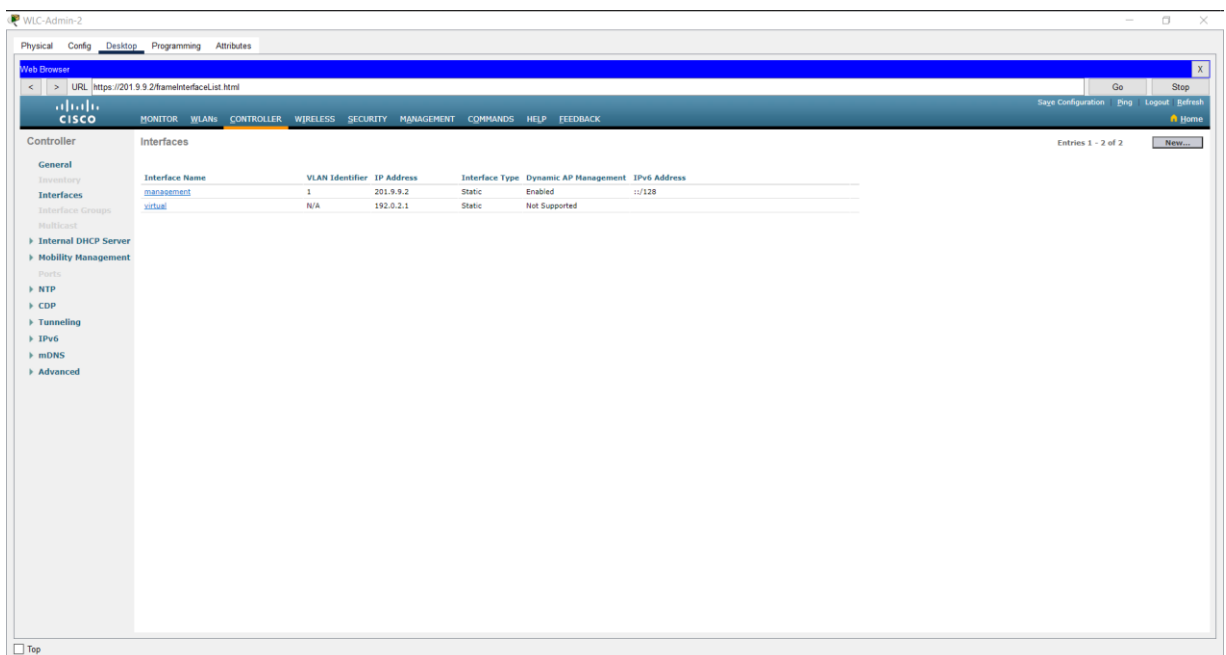


Рисунок 3.31 – Перегляд інформації про інтерфейси WLC

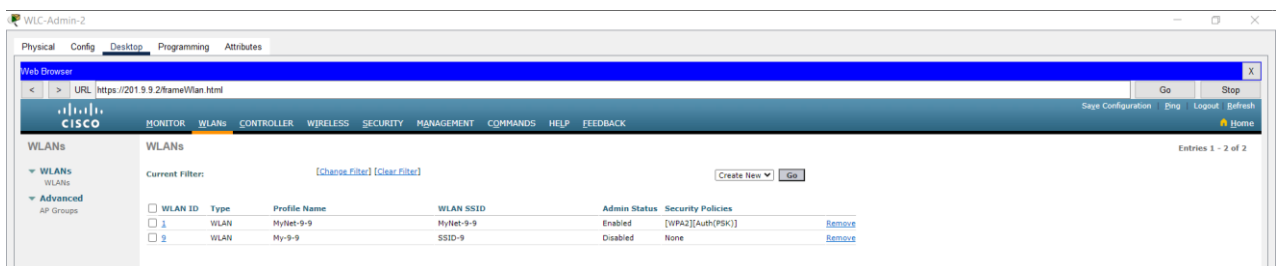


Рисунок 3.32 – Перегляд інформації про створені WLANs WLC

Перейдемо до перевірки налаштованих протоколів NTP, NAT, і Syslog щоб переконатися, що всі компоненти мережі працюють коректно та синхронізовано, а також для виявлення та усунення можливих проблем у конфігурації.

```
R-9-9-0#show ntp stat
Clock is synchronized, stratum 2, reference is 202.9.9.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E8179589.00000127 (19:42:1.295 UTC Fri Jun 23 2023)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 11.92 msec, peer dispersion is 0.00 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system poll
interval is 4, last update was 5 sec ago.
R-9-9-0#
```

Рисунок 3.33 – Перевірка роботи протоколу NTP

```
R-9-9-0#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 7 messages logged, xml disabled,
filtering disabled
Monitor logging: level debugging, 7 messages logged, xml disabled,
filtering disabled
Buffer logging: disabled, xml disabled,
filtering disabled

Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
Trap logging: level informational, 7 message lines logged
Logging to 202.9.9.2 (udp port 514, audit disabled,
authentication disabled, encryption disabled, link up),
7 message lines logged,
0 message lines rate-limited,
0 message lines dropped-by-MD,
xml disabled, sequence number disabled
filtering disabled
R-9-9-0#
```

Рисунок 3.34 – Перевірка роботи логування протоколу Syslog

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

```

R-9-9-0#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
udp  200.9.9.1:123      202.9.9.2:123    200.9.9.4:123     200.9.9.4:123
udp  200.9.9.1:67       200.9.9.1:67     255.255.255.255:68 255.255.255.255:68
R-9-9-0#

```

Рисунок 3.35 – Перевірка роботи протоколу NAT

Висновки до третього розділу:

Протягом даного розділу, було виконано вибір обладнання для створення мережі, а саме: комутаторів, маршрутизаторів та версії програмного забезпечення даних пристроїв; також було реалізовано раніше спроектовану мережу та виконано налаштування необхідних та додаткових технологій, таких як: динамічна маршрутизація, маршрутизація між VLAN, DHCP, та налаштування захисту з допомогою WPA та SSH, а також виконано налаштування протокол маршрутизації EIGRP, протокол мережевого часу NTP, протокол NAT і протокол Syslog.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

ВИСНОВКИ

У даному кваліфікаційній роботі було досліджено роботу динамічної маршрутизації та маршрутизації між VLAN, підвищений захист, а також побудовано локальну мережу організації з використанням даних технологій.

Створена мережа має 2 підмереж з можливістю розширення, використано 1 маршрутизатор та 4 комутаторів.

У першому розділі детально досліджено принципи побудови та функціонування технологій та протоколів, які використовуються для створення захищених локальних мереж. Розглянуто технології DHCP, SSH, WPA2-TKIP та інші. Визначено їхні переваги, недоліки та можливості застосування у корпоративних мережах. Зроблено висновок, що правильно налаштовані технології забезпечують високий рівень безпеки та надійності мережі.

У другому розділі проведено проектування фізичної топології мережі, розроблено систему IP-адресації, спроектовано підсистеми мережного захисту, такі як: доступ за користувачами та базовий захист, віддалений доступ та захист точок доступу Wi-Fi. Також у розділі розглянуто основні загрози для мережі, такі як шкідливе програмне забезпечення, фішинг, атаки за допомогою соціальної інженерії, неправильно налаштовані порти та служби.

Протягом останнього, третього розділу, було виконано вибір обладнання для створення мережі, а саме: комутаторів, маршрутизаторів та версії програмного забезпечення даних пристроїв; також було реалізовано раніше спроектовану мережу та виконано налаштування необхідних та додаткових технологій, таких як: динамічна маршрутизація, маршрутизація між VLAN, DHCP, та налаштування захисту з допомогою WPA та SSH, а також виконано налаштування протокол маршрутизації EIGRP, протокол мережевого часу NTP, протокол NAT і протокол Syslog.

Результатом виконання даної кваліфікаційної роботи стала функціонуюча та налагоджена локальна мережа організації, яку можна використовувати у житті.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Курси CCNAv7: Switching, Routing, and Wireless Essentials та CCNAv7: Enterprise Networking, Security, and Automation [Електронний ресурс] / Cisco – 2023. – Режим доступу до ресурсу: <https://www.netacad.com/portal/learning>
2. Cisco Catalyst 2960 Series Switches [Електронний ресурс] / Cisco – 2023. – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/switches/catalyst-2960-series-switches/series.html>
3. Cisco 2911 Integrated Services Router [Електронний ресурс] / Cisco – 2023. – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/routers/2911-integrated-services-router-isr/model.html>
4. IP Addressing: DHCP Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) [Електронний ресурс] / Cisco – 2023. – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/xs-3se/3850/dhcp-xe-3se-3850-book/config-dhcp-server.html
5. Computer Network Tutorials [Електронний ресурс] / GeeksForGeeks – 2023. – Режим доступу до ресурсу: <https://www.geeksforgeeks.org/computer-network-tutorials/?ref=ghm>
6. Configure SSH on Routers and Switches [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html>
7. Азаров О. Д. Комп'ютерні мережі: навчальний посібник / О. Д. Азаров, С. М. Захарченко, О. В. Кадук. – Вінниця : Вінницький Національний Технічний Університет, 2013. – 371 с. - ISBN 978-966-641-543-4
8. Особливості побудови локальних мереж [Електронний ресурс] – Режим доступу до статті: <http://studopedia.org/13-100846.html>

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

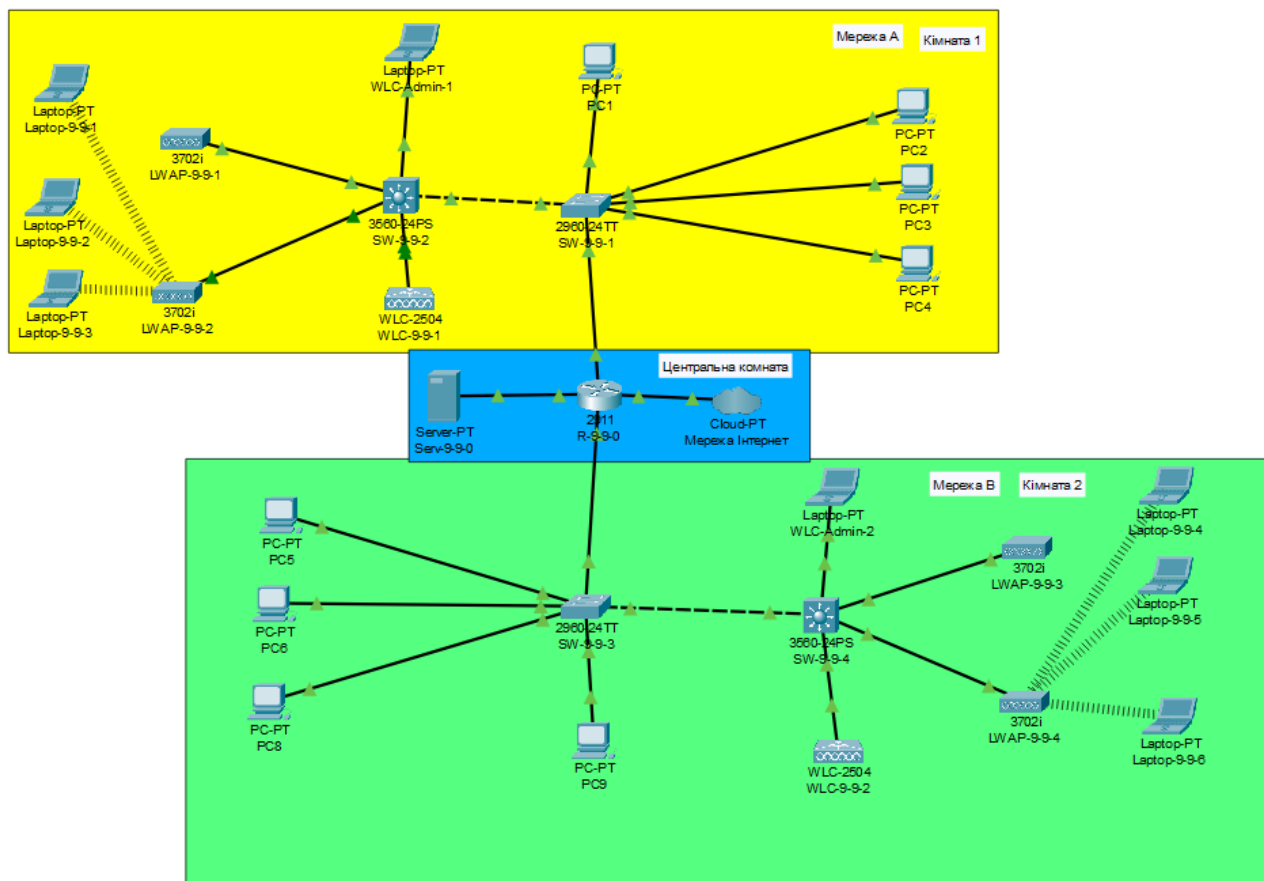
9. Олифер Виктор Григорьевич. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. / В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2010. – 944 с. – ISBN 978-5-49807-389-7.
10. Колисниченко Денис Николаевич. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание / Д. Н. Колисниченко. – СПб.: Наука и Техника, 2004. – 400 с. – ISBN 5-94387-160-8.
11. Таненбаум Э. Компьютерные сети. 5-е изд. / Э. Таненбаум. – СПб.: Питер, 2012. – 992 с. – ISBN 978-5-459-00342-0
12. Заика А. Компьютерные сети. / А. Заика. - М.: Олма-Пресс, 2006. — 448 с. – ISBN 5-224-05419-2
13. Основы компьютерных сетей: учеб. пособие / Б. Д. Виснадул, С. А. Лупин. С. В. Сидоров, П. Ю. Чумаченко / Под ред. Л.Г. Гагариной. М.: ИД «Форум»: ИНФРА-М. 2007. – 272 с. – ISBN 5-8199-0294-7
14. Семенов Андрей Борисович. Проектирование и расчет структурированных кабельных систем и их компонентов / А. Б. Семенов. – М.: ДМК Пресс; М.: Компаний АйТи, 2003. – 416+16 с. – ISBN 5-94074-210-6.
15. Кузьменко, Н.Г. Комп'ютерні мережі і мережеві технології / Н.Г. Кузьменко. - СПб.: Наука і техніка, 2013. - 368 с.
16. Столлінгс, В. Комп'ютерні мережі, протоколи і технології Інтернету / В. Столлінгс. - СПб.: BHV, 2005. - 832 с.
17. Основы организации сетей Cisco, том 1, испр. изд. : Пер. с англ. — М. : Издательский дом "Вильямс", 2004. — 512 с. : ил. — Парал. тит. англ.

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

ДОДАТКИ

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

Проект локальної мережі організації



Коржовський В.В.

Трокоз Є.М.

Арк.

ККІКБ<.КР.Б – 125 – 07 – ПЗ

70

Змн.

Арк.

№ докум.

Підпис

Дата

Технічні специфікації маршрутизатора Cisco 2911/K9

Код продукту	Cisco 2911/K9
Стелажні блоки	2RU
Інтерфейси	3 вбудованих порти 10/100/1000 Ethernet (тільки RJ-45)
Слот(и) розширення	1 слот для сервісного модуля
	1 слот для внутрішнього сервісного модуля
	2 слоти для вбудованого цифрового сигнального процесора (DSP)
	4 слоти для розширених високошвидкісних інтерфейсних плат WAN
ОПЕРАТИВНА ПАМ'ЯТЬ	512 МБ (встановлено) / 2 ГБ (макс.)
Флеш-пам'ять	256 МБ (встановлено) / 8 ГБ (макс.)
Розміри	43,8 см x 30,5 см x 8,9 см
Вага упаковки	16,15 кг

Технічні специфікації комутатора Cisco Catalyst 2960-24TTL

Код продукту	WS-C2960-24TT-L
Тип корпусу	Монтаж у стійку - 1U
Набір функцій	LAN Base
Інтерфейси висхідної лінії зв'язку	2 x 10/100/1000 TX uplink
Порти	24 x Ethernet 10/100 порти
Пропускна здатність	6,5 МПП
Ємність об'єднувальної плати	16 Гбіт/с
DRAM	16 МБ
Розміри	1,73 x 17,5 x 9,3 дюйма.
Вага упаковки	8,15 кг

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

Нижче представлені конфігураційні файли пристроїв мережі

!	!	\$1\$mERr\$3akjomZu5CoJg RwkR0qHs1
version 15.1	ip dhcp pool R_1	username userR0 secret 5 \$1\$mERr\$\$5tItBsSTHp4n 1WbqjsM0
service timestamps log datetime msec	network 200.9.9.0 255.255.255.0	!
service timestamps debug datetime msec	default-router 200.9.9.1	!
no service password- encryption	dns-server 1.1.1.1	license udi pid CISCO2911/K9 sn FTX1524FR58-
!	ip dhcp pool R_2	
hostname R-9-9-0	network 201.9.9.0 255.255.255.0	!
!	default-router 201.9.9.1	!
logging userinfo	dns-server 2.2.2.2	!
!	clock timezone EEST 2	!
!	!	!
enable secret 5 \$1\$mERr\$M8hiclNzJMod2 7zv5MBjW.	!	!
!	!	!
!	no ip cef	!
ip dhcp excluded-address 200.9.9.1 200.9.9.2	no ipv6 cef	ip domain-name my.net
ip dhcp excluded-address 201.9.9.1 201.9.9.2	!	!
ip dhcp excluded-address 200.9.9.3 200.9.9.4	!	spanning-tree mode pvst
ip dhcp excluded-address 201.9.9.3 201.9.9.4	username adminR0 privilege 15 secret 5 \$1\$mERr\$vTbHul1N28cEp 8lkLqr0f/	!
ip dhcp excluded-address 200.9.9.30	username ingenerR0 privilege 5 secret 5	!

Коржовський В.В.

Трокоз Є.М.

Змн.

Арк.

№ докум.

Підпис

Дата

ККІКБ<.КР.Б – 125 – 07 – ПЗ

Арк.

73

!	!	access-list 1 permit 202.9.9.0 0.0.0.255
!	interface FastEthernet0/0/2	!
interface GigabitEthernet0/0	switchport mode access	!
ip address 200.9.9.1 255.255.255.0	!	!
ip nat outside	interface FastEthernet0/0/3	!
duplex auto	switchport mode access	!
speed auto	!	logging 202.9.9.2
!	interface Vlan1	line con 0
interface GigabitEthernet0/1	no ip address	!
ip address 201.9.9.1 255.255.255.0	shutdown	line aux 0
ip nat inside	!	!
duplex auto	router eigrp 1	line vty 0 4
speed auto	network 200.9.9.0	login local
!	network 201.9.9.0	transport input ssh
interface GigabitEthernet0/2	network 202.9.9.0	transport output ssh
ip address 202.9.9.1 255.255.255.0	!	!
ip nat inside	ip nat inside source list 1	!
duplex auto	interface GigabitEthernet0/0	ntp authentication-key 1111 md5 08701D1F58 7
speed auto	overload	ntp trusted-key 1111
!	ip classless	ntp server 202.9.9.2 key 1111
interface FastEthernet0/0/0	!	ntp update-calendar
switchport mode access	!	!
!	access-list 1 permit 200.9.9.0 0.0.0.255	end
interface FastEthernet0/0/1	access-list 1 permit 201.9.9.0 0.0.0.255	!
switchport mode access		

```

version 15.0                                !                                line con 0

service timestamps log                       spanning-tree mode pvst                !
datetime msec

service timestamps debug                     spanning-tree extend                  line vty 0 4
datetime msec                               system-id                             login local

no service password-                        !                                transport input ssh
encryption                                  interface FastEthernet0/1            transport output ssh

!                                           !                                line vty 5 15

hostname SW-9-9-1                           interface FastEthernet0/2            login

!                                           !                                !

enable secret 5                             ...                                !
$1$mERr$M8hiclNzJMod2                     !                                !
7zv5MBjW.                                   !                                ntp trusted-key 1111

!                                           interface FastEthernet0/24          ntp server 202.9.9.2 key
!                                           !                                1111
!                                           interface GigabitEthernet0/1        !

clock timezone EEST 2                       !                                end

!                                           interface GigabitEthernet0/2        !

ip domain-name my.net                       !                                !

!                                           interface Vlan1                     !

username adminSW1 secret                    ip address 200.9.9.3                version 12.2(37)SE1
5                                           255.255.255.0                      service timestamps log
$1$mERr$vTbHul1N28cEp                       !                                datetime msec
8lkLqr0f/

username ingenerSW1                        ip default-gateway                  service timestamps debug
secret 5                                     200.9.9.1                          datetime msec
$1$mERr$3akjomZu5CoJg                       !                                no service password-
RwkR0qHs1                                    logging 202.9.9.2                   encryption

username userSW1 secret 5                  !                                !
$1$mERr$$5tItBsSTHp4n                       !                                !
1WbqjsM0                                     !                                hostname SW-9-9-2

!                                           !                                !

!                                           !

```

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		75

```

logging userinfo                                !                                !

!                                !                                ip default-gateway
200.9.9.1

enable secret 5                                ip domain-name my.net
$1$mERr$M8hiclNzJMod2                          !                                ip classless
7zv5MBjW.                                       !

!                                !

!                                spanning-tree mode pvst

!                                !

!                                !

clock timezone EEST 2                          !                                !

!                                !

!                                !

!                                !

!                                !

!                                !

!                                interface FastEthernet0/1

!                                !

!                                logging 202.9.9.2

username adminSW2                             interface FastEthernet0/2
privilege 15 secret 5                          !                                line con 0
$1$mERr$vTbHul1N28cEp                         !                                !
8lkLqr0f/                                     ...

username userSW2 secret 5                     !                                line aux 0
$1$mERr$S/5tItBsSTHp4n                       !                                !
1WbqjsM0

!                                interface FastEthernet0/24

!                                !                                line vty 0 4

!                                !                                login local

!                                interface GigabitEthernet0/1

!                                !                                transport input ssh

!                                !                                transport output ssh

!                                interface GigabitEthernet0/2

!                                !

!                                !

!                                interface Vlan1

!                                !

!                                ip address 200.9.9.4
255.255.255.0

```

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		76

```

ntp authentication-key 1111      username adminSW3 secret
md5 08701D1F58 7                5
                                $1$mERr$vTbHul1N28cEp
ntp trusted-key 1111             8lkLqr0f/      ip address 201.9.9.3
                                255.255.255.0

ntp server 202.9.9.2 key         username ingenerSW3      !
1111                             secret 5
                                $1$mERr$3akjomZu5CoJg
ntp update-calendar              RwkR0qHs1      ip default-gateway
                                201.9.9.1

!                                username userSW3 secret 5      !
                                $1$mERr$S/5tItBsSTHp4n
end                               1WbqjsM0      logging 202.9.9.2

                                !                                !

!                                !                                !

version 15.0                     !                                !

service timestamps log           spanning-tree mode pvst      line con 0
datetime msec

                                spanning-tree extend          !
service timestamps debug        system-id
datetime msec

                                !                                line vty 0 4

no service password-            interface FastEthernet0/1      login local
encryption

                                !                                transport input ssh

!                                !                                transport output ssh

hostname SW-9-9-3               interface FastEthernet0/2      line vty 5 15

!                                !                                login

enable secret 5                 ...                                !
$1$mERr$M8hiclNzJMod2          !                                !
7zv5MBjW.                      !                                !

!                                interface FastEthernet0/24      !

!                                !                                !

!                                interface GigabitEthernet0/1      ntp trusted-key 1111

!                                ntp server 202.9.9.2 key
clock timezone EEST 2           1111

!                                interface GigabitEthernet0/2      !

ip domain-name my.net           !                                end

!                                interface Vlan1

```

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

!	username ingenerSW4	interface FastEthernet0/2
version 12.2(37)SE1	privilege 5 secret 5	!
	\$1\$mERr\$3akjomZu5CoJg	
	RwkR0qHs1	
service timestamps log		...
datetime msec	username userSW4 secret 5	!
	\$1\$mERr\$\$S/5tItBsSTHp4n	
service timestamps debug	1WbqjsM0	
datetime msec		interface FastEthernet0/24
	!	
no service password-		!
encryption	!	
		interface GigabitEthernet0/1
!	!	!
hostname SW-9-9-4	!	
		interface GigabitEthernet0/2
!	!	
		!
logging userinfo	!	
		interface Vlan1
!	!	
		ip address 201.9.9.4
enable secret 5	!	255.255.255.0
\$1\$mERr\$M8hiclNzJMod2		
7zv5MBjW.	!	!
!	!	ip default-gateway
		201.9.9.1
!	ip domain-name my.net	
		ip classless
!	!	
		!
clock timezone EEST 2	!	
		ip flow-export version 9
!	spanning-tree mode pvst	!
!	!	
		!
!	!	
		!
!	!	
		!
!	!	
		!
username adminSW4	!	
privilege 15 secret 5		!
\$1\$mERr\$vTbHul1N28cEp	interface FastEthernet0/1	
8lkLqr0f/		!
	!	

logging 202.9.9.2

line con 0

!

line aux 0

!

line vty 0 4

login local

transport input ssh

transport output ssh

!

!

!

ntp authentication-key 1111
md5 08701D1F58 7

ntp trusted-key 1111

ntp server 202.9.9.2 key
1111

ntp update-calendar

!

end

		Коржовський В.В.			ККІКБ<.КР.Б – 125 – 07 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		79