Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Система управління Wi-Fi радіоспотами з використанням системи RADIUS
Назва теми

КвРКІ. 190214.19.02.34 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Виконав: студент IV курсу, група КІ2–19–2 ______ В. В. Заєць
Підпис Ініціали, прізвище

Керівник ______ О. В. Іванов
Підпис, дата Ініціали, прізвище

Нормоконтролер ______ С.М. Лисенко
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри комп'ютерної інженерії та інформаційних систем ______ Т.О. Говорущенко
Підпис Ініціали, прізвище

«26» червня 2023 р.

Хмельницький 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформамійних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Освітній рівень бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма «комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

"11" 01 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Зайцю Віталію Вікторовичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Система управління Wi-Fi радіоспотами з використанням системи RADIUS

Керівник проекту (роботи) Іванов О.В., к.т.н., доцент.

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 01.03.2023 р. № 5

2. Строк подання студентом проекту (роботи) на кафедру 01.06.2023 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Дослідження предметної області та постановка задачі

Моделювання та проєктування системи управління

Апаратна реалізація системи управління

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Система моніторингу та аналізу системи RADIUS

Система вбудованого RADIUS сервера

Побудова ER-діаграми

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийн
Нормоконтроль	Лисенко С.М., професор кафедри КІІС		
Антиплагіат	Нічепорук А.О., доцент кафедри КІІС		

7. Дата видачі завдання «__01__»________03__________2023 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Приміт
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	20.02.2022	виконан
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.03.2023	виконан
3	Робота над розділом 1 – дослідження предметної області та постановка задачі	10.03.2023	виконан
4	Робота над розділом 2 – моделювання та проєктування системи управління	20.04.2023	виконан
5	Робота над розділом 3 – апаратна реалізація системи управління	30.04.2023	виконан
6	Оформлення пояснювальної записки згідно вимог	24.05.2023	виконан
7	Попередній захист ВКР	25.05.2023	виконан
8	Захист ВКР на засіданні ЕК	Червень 2023 року	

Студент ______________ В.В. Заєць
Підпис Ініціали, прізвище

Керівник проекту (роботи) ______________ О. В. Іванов
Підпис Ініціали, прізвище

№ рядка	Формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ 190247.19.02.26 ПЗ	Пояснювальна записка	61		
			Графічні матеріали			
2		КвРКІП 190362.17.03.09 Е8	Логічні схеми алгоритмів	1		
3		КвРКІП 190362.17.03.09 Е8	Мікрокомандна схема та граф-схема переходів автомату Мура	1		
4		КвРКІП 190362.17.03.09 Е2	Схема електрична функціональна операційного автомату	1		

КвРКІ 190214.19.05.34 ВП

Зм	Арк	№ докум	Підпис	Дата
Розробив		Засць	Засць	26.06
Перевір.		Іванов		26.06
Н. контр.		Лисенко		26.06
Затв.		Говорущенко		26.06

Відомість проекту

Літера	Аркуш	Аркушів
У	1	1

ХНУ, КІ2-19-2

АНОТАЦІЯ

Автор роботи: Заєць Віталій Вікторович.

Керівник роботи: Іванов Олексій Валентинович.

Пояснювальна записка: 61 с., 32рис., 3 дод., 40 джерела.

Графічна частина: 3 креслень.

Метою роботи є розробка системи управління Wi-Fi радіоспотами з використанням системи RADIUS.

Об'єктом дослідження є програмно-технічний (апаратний) засіб – Система управління Wi-Fi радіоспотами з використанням системи RADIUS.

Предметом дослідження є формалізований опис та схеми системи управління WI-FI радіоспотами з використанням системи RADIUS.

Практичне значення має змодельована, спроєктована та реалізована система управління WI-FI радіоспотами з використанням системи RADIUS.

Заєць — 23.06.23

Підпис студента — Дата

ЗМІСТ

					КвРКІ 190214.19.05.34 ПЗ			
Зм.	Арк.	№докум.	Підпис	Дата				
Виконав		Засць В.В.		26.06	Система управління Wi-Fi радіоспотами з використанням системи RADIUS Пояснювальна записка	Літера	Аркуш	Аркушів
Перевір.		Іванов О.В.		26.06		у		X
Н.контр.		Лисенко С.М.		26.06		ХНУ КІ2-19-2		
Затвер.		Говорущенко Т.О.		26.06				

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ISE- Cisco Identity Services Engine

IAM- управління ідентифікацією та доступом

RADIUS (Remote Authentication Dial-In User Service)

AAA (authentication authorization accounting)

Міб (MIB - Management Information Base)

(Network Access Server - NAS)

MD5 (Mes-sa-ge-Di-gest al-go-rithm 5)

ВСТУП

У сучасному світі широке розповсюдження бездротових мереж зробило необхідним ефективне управління точками доступу Wi-Fi. Однією з основних проблем, з якою стикаються мережеві адміністратори, є забезпечення безпечного і надійного доступу до бездротових мереж. Це призвело до розробки різних технологій і протоколів для поліпшення управління і безпеки бездротових мереж, таких як система RADIUS (Remote Authentication Dial-In User Service). Система RADIUS забезпечує централізовану аутентифікацію, авторизацію та облік доступу до мережі, що робить її важливим інструментом для управління Wi-Fi мережами. У цьому проекті ми маємо на меті розробити систему управління точками доступу Wi-Fi, яка використовує систему RADIUS для покращення безпеки та управління бездротовими мережами.

Запропонована система управління точками доступу Wi-Fi має на меті спростити управління точками доступу Wi-Fi шляхом автоматизації багатьох завдань, які традиційно виконуються мережевими адміністраторами вручну. Використовуючи систему RADIUS як основний механізм аутентифікації та авторизації, система може гарантувати, що доступ до мережі надається лише авторизованим користувачам. Це не лише підвищує безпеку бездротової мережі, але й покращує загальний користувацький досвід за рахунок зменшення часу і зусиль, необхідних для управління точками доступу Wi-Fi.

Система буде масштабованою та адаптованою, що зробить її придатною для розгортання в різних організаціях, таких як школи, університети та корпоративні середовища. Система також надаватиме можливості моніторингу та звітності в режимі реального часу, що дозволить мережевим адміністраторам відстежувати використання мережі та виявляти потенційні загрози безпеці.

В цілому, система управління точками доступу Wi-Fi з використанням системи RADIUS має на меті забезпечити комплексне рішення для управління точками доступу Wi-Fi, покращити безпеку та управління бездротовими мережами, а також підвищити загальну зручність роботи користувачів.

Розробка цієї системи управління точками доступу Wi-Fi з використанням системи RADIUS має потенціал докорінно змінити спосіб управління бездротовими мережами в організаціях. Надаючи комплексне та автоматизоване рішення для управління точками доступу Wi-Fi, система дозволить мережевим адміністраторам зосередитися на інших важливих завданнях, таких як планування мережевої інфраструктури та моніторинг безпеки. Зрештою, запропонована система покращить загальну безпеку, надійність та управління мережами Wi-Fi, що принесе користь як організаціям, так і кінцевим користувачам.

1. ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Змістовний аналіз предметної області, її структурних та функціональних особливостей

Метою роботи над темою "Система управління радіоточкою Wi-Fi з використанням системи RADIUS" є розробка системи, яка може ефективно управляти та контролювати доступ до мережі Wi-Fi на певній території або в певному місці. Система використовує протокол RADIUS (Remote Authentication Dial-In User Service), який є широко використовуваною системою аутентифікації та обліку для управління доступом до мережі.

Система призначена для управління точками доступу Wi-Fi, які є певними областями в межах більшої мережі Wi-Fi. Використовуючи систему RADIUS, система управління може контролювати доступ до цих радіоточок на основі автентифікації та авторизації користувачів (рис. 1.1). Це може допомогти запобігти несанкціонованому доступу до мережі, забезпечити мережеву безпеку і підвищити загальну продуктивність і ефективність мережі.

RADIUS (Remote Authentication Dial-In User Service) - це протокол аутентифікації, авторизації та обліку (AAA), який використовується для керування доступом користувачів до мережі. Система RADIUS дозволяє здійснювати централізоване керування доступом користувачів до різних ресурсів мережі, таких як мережеві порти, сервери, VPN-з'єднання тощо. Завдяки системі RADIUS можна контролювати ідентифікацію користувача, його права доступу та час знаходження в мережі.

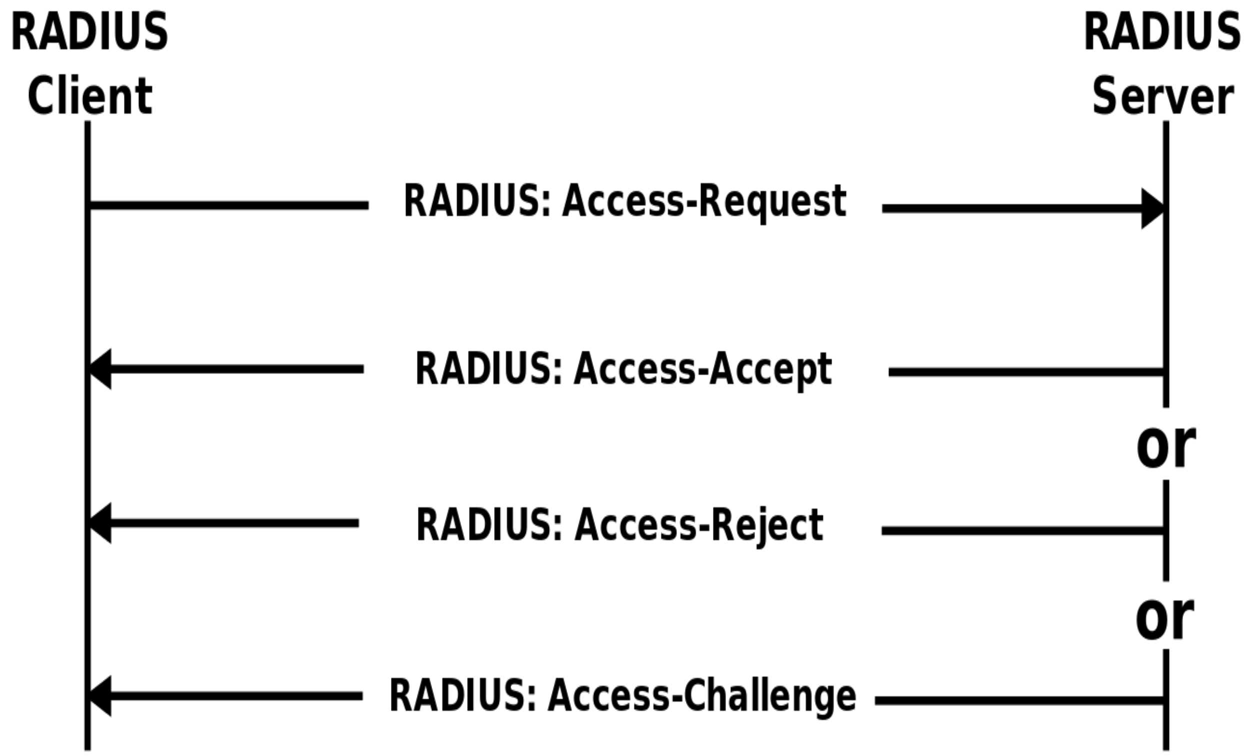


Рисунок 1.1 - Аутентифікація та авторизація через RADIUS-сервер

Система також може включати такі функції, як автентифікація користувачів, відстеження користувачів, моніторинг використання та звітування, які можуть надати цінну інформацію та уявлення про моделі використання мережі та допомогти оптимізувати продуктивність мережі. Крім того, система може використовуватися в різних умовах, таких як публічні точки доступу Wi-Fi, корпоративні мережі та навчальні заклади. Система RADIUS (рис. 1.2) складається з трьох основних компонентів: сервера RADIUS, клієнтської програми RADIUS і бази даних користувачів. Сервер RADIUS відповідає за аутентифікацію користувача та прийняття рішення про надання доступу до мережі. Клієнтська програма RADIUS встановлює зв'язок з сервером RADIUS та передає запити на аутентифікацію користувачів. База даних користувачів містить інформацію про ідентифікацію користувача та його права доступу.

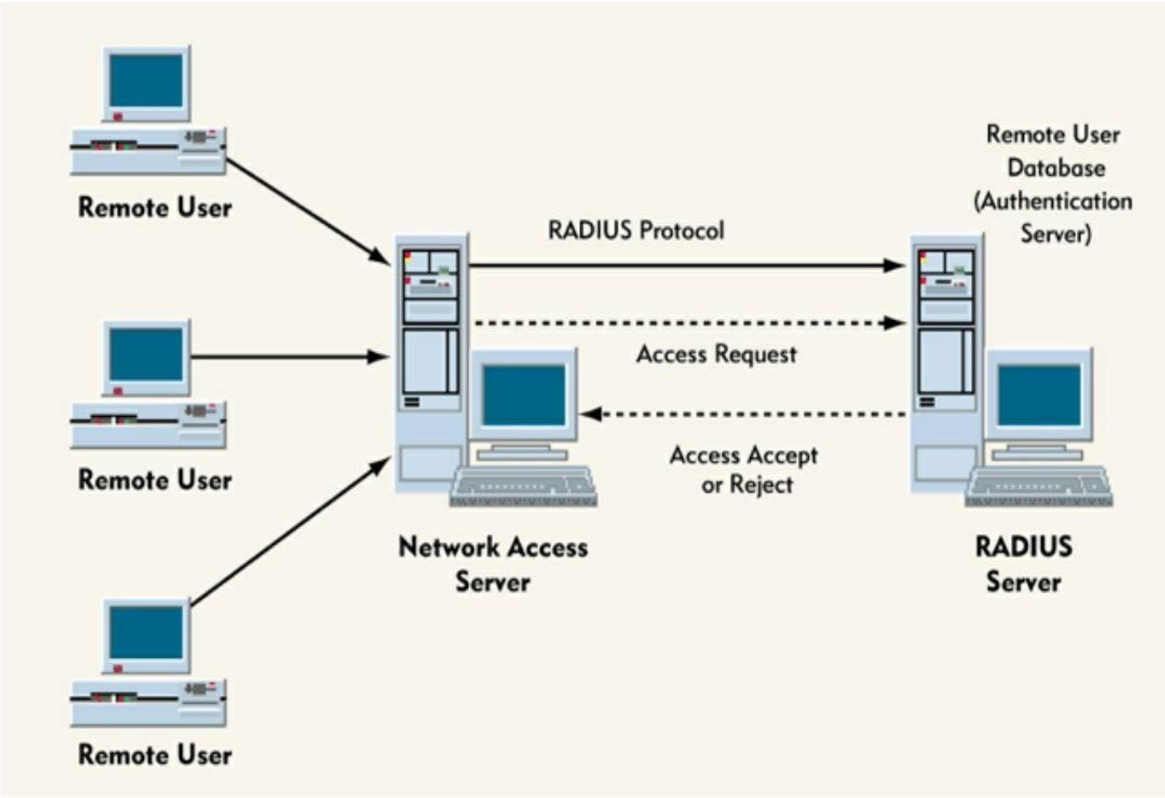


Рисунок 1.2 - Система RADIUS

Застосування системи управління WIFI радіоспотами з використанням системи RADIUS дозволяє забезпечити контроль доступу користувачів до мережі з використанням ідентифікаторів і паролів, а також встановити різні рівні доступу для різних категорій користувачів. Однак, при використанні цієї технології, можуть виникати ряд проблем і завдань, серед яких можна виокремити наступні:

1. Безпека мережі: використання паролів для авторизації користувачів може стати неефективним у разі, якщо хакер отримує доступ до паролів, тоді він може безперешкодно користуватись мережею. Тому необхідно забезпечити додаткову захист мережі від несанкціонованого доступу, наприклад, за допомогою шифрування мережевого трафіку.

2.Стійкість мережі: використання системи RADIUS дозволяє забезпечити більш ефективний контроль доступу користувачів до мережі, проте при великому потоці користувачів, система може стати недоступною. Тому необхідно забезпечити стійкість мережі та високу продуктивність системи.

3.Налаштування мережі: для ефективної роботи системи управління WIFI радіоспотами з використанням системи RADIUS, необхідно правильно налаштувати мережу та точки доступу Wi-Fi. Це може бути складним завданням для некваліфікованого персоналу.

4.Вартість: використання системи управління WIFI радіоспотами з використанням системи RADIUS може бути досить витратним завданням.

5.Інтеграція з іншими системами: у разі, якщо компанія використовує різні системи управління мережами, виникає проблема їх інтеграції з системою RADIUS. Необхідно забезпечити сумісність систем та їх взаємодію

6.Підтримка та обслуговування: для ефективної роботи системи управління WIFI радіоспотами з використанням системи RADIUS необхідна постійна підтримка та обслуговування з боку кваліфікованого персоналу.

1.2 Порівняльний аналіз платформ, їх недоліки та переваги

На сьогоднішній день існує декілька рішень системи управління WIFI радіоспотами з використанням системи RADIUS. Розглянемо декілька з них та порівняємо їх переваги:

FreeRADIUS - це широко використовувана реалізація протоколу RADIUS (Remote Authentication Dial-In User Service) з відкритим вихідним кодом. Це високопродуктивний, модульний і масштабований сервер, який використовується для автентифікації мережевих користувачів і надання послуг авторизації та обліку.

FreeRADIUS підтримує широкий спектр методів автентифікації, включаючи PAP (Password Authentication Protocol), CHAP (Challenge-Handshake Authentication Protocol), MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol), EAP (Extensible Authentication Protocol) та багато інших. Він також підтримує різні внутрішні бази даних, такі як MySQL, PostgreSQL, Oracle і LDAP.

Однією з переваг FreeRADIUS є його гнучкість і можливість налаштування. Його можна налаштувати під широкий спектр мережевих налаштувань і сценаріїв автентифікації. Він також має високу масштабованість і може обробляти велику кількість одночасних запитів на автентифікацію.

FreeRADIUS надає комплексну функціональність реєстрації та обліку, що дозволяє мережевим адміністраторам відстежувати активність користувачів і створювати звіти про використання. Він також підтримує різні методи обліку, включаючи одночасне використання, облік на основі часу та обсягу.

В цілому, FreeRADIUS (рис. 1.2) є потужним і універсальним рішенням для автентифікації та авторизації, яке широко використовується на підприємствах, в мережах провайдерів послуг та освітніх мережах. Завдяки відкритому вихідному коду та активній спільноті розробників FreeRADIUS є популярним вибором для організацій, які шукають економічно ефективний RADIUS-сервер, що налаштовується.

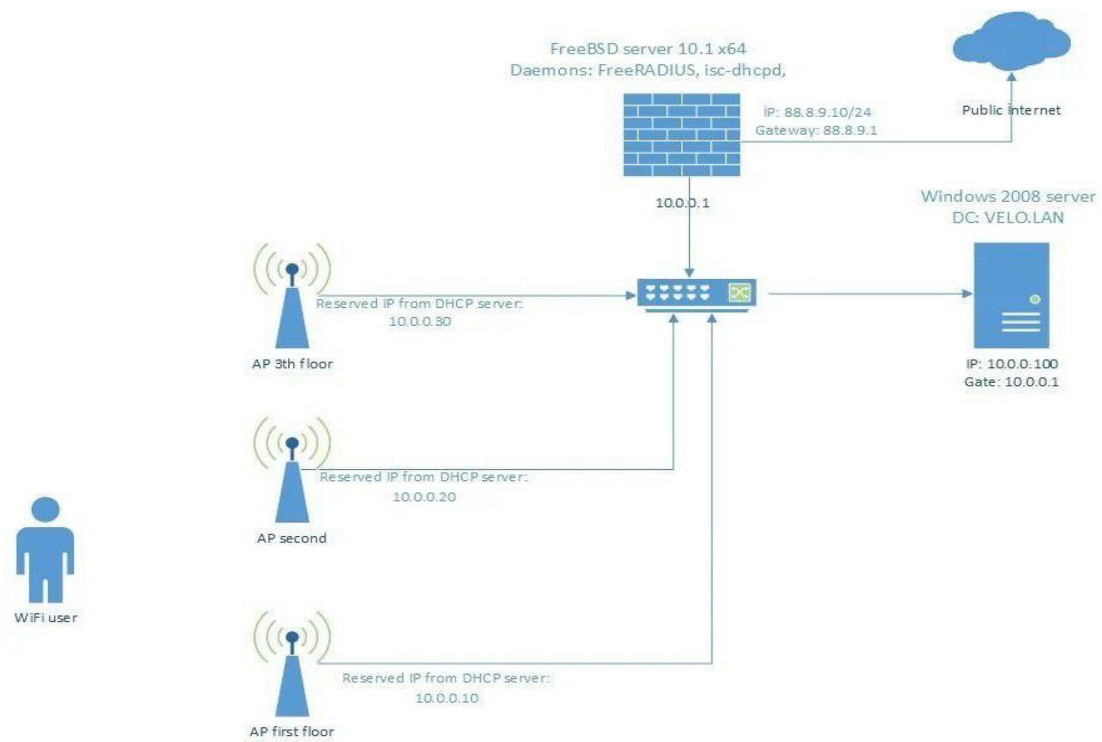


Рисунок 1.2 - FreeRADIUS

Cisco Identity Services Engine (ISE) (рис.1.3) - це продукт для мережевого адміністрування, який забезпечує безпечний доступ до мережевих ресурсів. Це потужне і комплексне рішення для управління ідентифікацією та доступом (IAM), яке дозволяє IT-командам впроваджувати політики безпеки у всій мережевій інфраструктурі.

ISE підтримує широкий спектр методів автентифікації та авторизації, включаючи RADIUS, TACACS+, 802.1X і SAML. Він також надає функції профілювання пристроїв, оцінки стану безпеки та гостьового доступу, що дозволяє IT-командам застосовувати політики на основі типу пристрою користувача, операційної системи та стану безпеки.

Однією з ключових особливостей ISE є система контролю доступу на основі політик. Вона дозволяє IT-командам визначати деталізовані політики на основі ідентичності користувача, типу пристрою, місцезнаходження, часу та інших факторів. Політики можуть застосовуватися до всієї мережевої інфраструктури, включаючи дротові та бездротові мережі, VPN і мережеві пристрої.

ISE також надає розширені можливості звітності та аналітики, що дозволяє IT-командам відстежувати і аналізувати активність користувачів, відповідність пристроїв і події безпеки. Він може генерувати докладні звіти про доступ користувачів, використання мережі та стан відповідності, допомагаючи організаціям відповідати нормативним вимогам і вимогам відповідності.

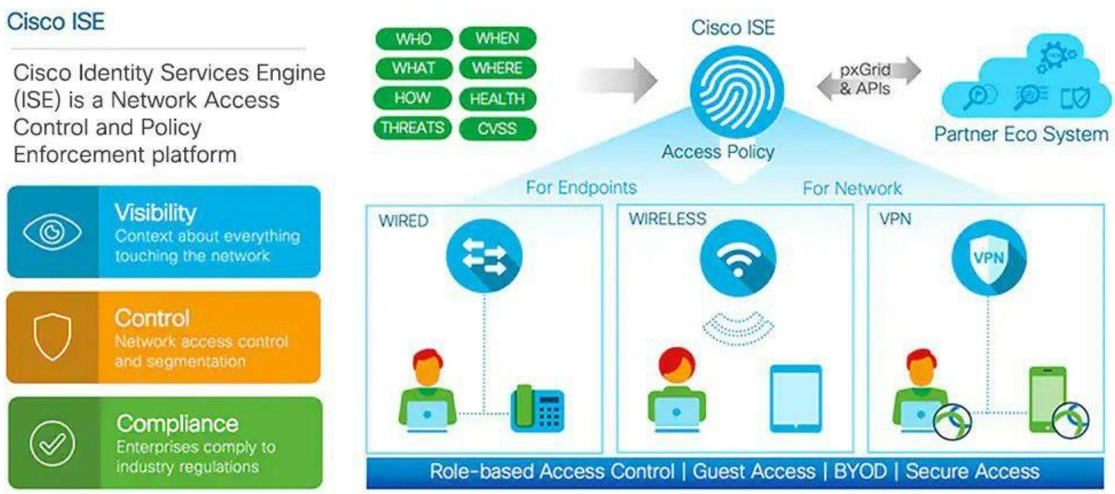


Рисунок 1.3 - Cisco Identity Services Engine

У порівнянні з іншими рішеннями, FreeRADIUS має переваги у відкритому коді та можливості використання на різних операційних системах. Cisco ISE є більш повноцінними системами управління мережею, що підтримують широкий спектр протоколів і функціональних можливостей. Вони забезпечують можливість автоматичної аутентифікації та авторизації користувачів, що значно спрощує процес управління доступом до мережі.

Cisco ISE також мають можливість інтеграції з іншими системами моніторингу та управління мережею, що дозволяє забезпечити єдину точку керування мережею. Тому в своїй роботі я буду користуватись послугами ISE.

Дослідження предметної області системи управління Wi-Fi радіоспотами з використанням системи RADIUS включає в себе аналіз функцій та можливостей, які ця система надає для управління і автентифікації користувачів у Wi-Fi мережі. Основною метою такого дослідження є визначення технологій, протоколів та процесів, які використовуються в системі управління Wi-Fi радіоспотами з RADIUS.

1.3 Основні етапи дослідження

Основні етапи дослідження можуть включати:

1. Огляд системи RADIUS: Дослідження протоколу RADIUS (Remote Authentication Dial-In User Service), що використовується для централізованої автентифікації, авторизації та обліку користувачів (рис.1.4). Розуміння архітектури, протоколів і процесів RADIUS дозволяє зрозуміти, як вона може бути використана для управління Wi-Fi радіоспотами.

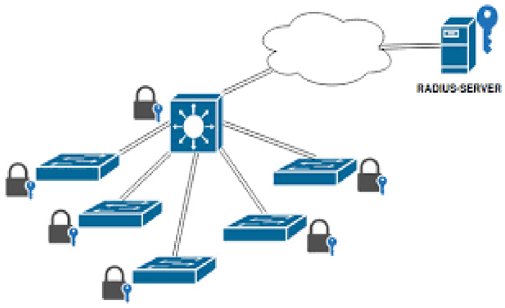


Рис.1.4 - централізована автентифікація користувачів

2. Управління Wi-Fi радіоспотами: Дослідження методів управління Wi-Fi радіоспотами, включаючи можливості налаштування параметрів мережі, керування доступом користувачів та моніторингу стану радіоспотів. Вивчення протоколів, таких як SNMP (Simple Network Management Protocol), може бути корисним для збору інформації про радіоспоти.

3. Інтеграція RADIUS і Wi-Fi: Вивчення можливостей і протоколів для інтеграції системи RADIUS з Wi-Fi радіоспотами. Дослідження можливостей автентифікації користувачів, яка базується на системі RADIUS, і налаштування параметрів безпеки для забезпечення захищеного доступу до Wi-Fi.

4. Протокол SNMP (рис.1.5) (Simple Network Management Protocol) є стандартним протоколом управління мережевими пристроями в тому числі у системі RADIUS.

Рис. 1.5 - протокол (Simple Network Management Protocol)

Він використовується для збору і моніторингу інформації про стан мережевих пристроїв, налаштування їх параметрів та керування ними. SNMP дозволяє централізовано взаємодіяти з різними пристроями, такими як маршрутизатори, комутатори, сервери, принтери і т. д.

Менеджер (SNMP Manager): Це програмне забезпечення або пристрій, який виконує функцію керування мережею. Він ініціює запити до агентів та обробляє отримані відповіді.

Агент (SNMP Agent): Це програмне забезпечення, що запущене на мережевому пристрої. Воно збирає інформацію про стан пристрою та відправляє її до менеджера при запитах.

Міб (MIB - Management Information Base): Це база даних, яка містить ієрархічно організовану колекцію об'єктів, що визначаються протоколом SNMP. Кожен об'єкт в Мібі має унікальний ідентифікатор та значення, яке може бути прочитане або змінене. SNMP трапи (SNMP Traps): Це повідомлення, яке відправляється агентом до менеджера, щоб повідомити про певну подію або помилку, яка виникла на пристрої.

Протокол SNMP використовується для віддаленого керування пристроями, отримання статистики про мережевий трафік (рис. 1.6), моніторингу ресурсів та виявлення помилок.

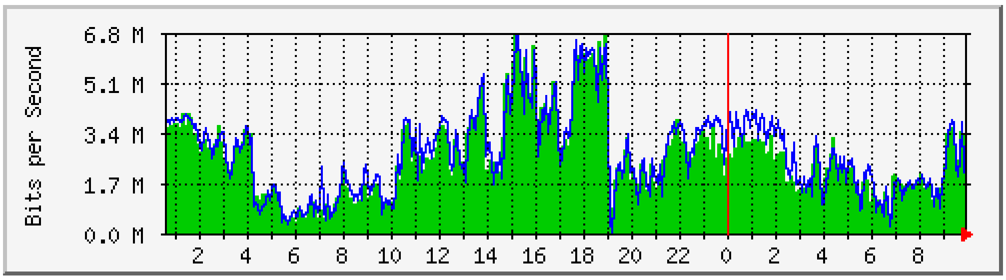


Рисунок 1.6 - графік мережевого трафіку

Він дозволяє мережним адміністраторам віддалено налаштовувати та керувати пристроями у мережі з одного центрального місця.

Переваги використання системи управління Wi-Fi радіоспотами з використанням системи RADIUS.

Централізована автентифікація і авторизація: RADIUS дозволяє централізовано автентифікувати та авторизувати користувачів, незалежно від їх місцезнаходження в мережі. Це означає, що користувачі можуть використовувати одні й ті ж облікові дані для доступу до різних Wi-Fi радіоспотів, спрощуючи процес аутентифікації та забезпечуючи єдиноцентрове керування доступом.

Удосконалена безпека: RADIUS надає можливість використовувати протоколи шифрування, такі як EAP (Extensible Authentication Protocol), для безпечної передачі облікових даних та інших чутливих даних між користувачем і сервером RADIUS. Це дозволяє забезпечити конфіденційність даних та запобігти несанкціонованому доступу до мережі.

Гнучкість та розширюваність: RADIUS підтримує широкий спектр методів аутентифікації, включаючи пароль, токен, сертифікати та багато інших. Він також може бути розширений для підтримки нових методів аутентифікації, які можуть виникнути в майбутньому. Це дає можливість вибирати найбільш підходящий метод аутентифікації для конкретного застосування.

Облік трафіку та моніторинг: RADIUS забезпечує можливість ведення обліку трафіку користувачів, зокрема кількості переданих даних та тривалості сеансів. Це дозволяє контролювати використання мережевого ресурсу і проводити моніторинг діяльності користувачів.

Протокол RADIUS був розроблений компанією Livingston Enterprises (конкретно Карлом Рігні/Carl Rigney) для віддаленого комутованого доступу через мережеві сервери доступу (Network Access Server - NAS) цієї компанії серії PortMaster до мережі internet. Пізніше, в 1997, протокол RADIUS був опублікований як RFC 2058 і RFC 2059. Поточні версії RFC 2865 (Remote Authentication Dial In User Service (RADIUS)) і RFC 2866 (RADIUS Accounting). Іноді замість поняття "мережевий сервер доступу" використовується інший: "віддалений сервер доступу" (Remote Access Server - RAS).

Термін Облік використаних мережевих ресурсів вже сам по собі досить інформативний. Первинними даними, які передаються по протоколу RADIUS, є обсяги вхідного і вихідного трафіків при передачі даних, і тривалість розмови і набраний номер при використанні IP телефонії. Крім визначених у протоколі стандартних атрибутів (параметрів), протокол передбачає можливість використання виробником обладнання (вендором) власних атрибутів. В англомовній літературі вони називаються Vendor Specific Attributes або VSA.

Під Аутентифікацією (рис.1.7) розуміється процес, що дозволяє ідентифікувати користувача за його даними, наприклад, за логіном (ім'я користувача, номер телефону і т. Д.) і паролю.

Авторизація - процес, протягом якого визначаються повноваження ідентифікованого користувача на доступ до певних мережевих ресурсів.

В даний час протокол RADIUS використовується для доступу до віртуальних приватних мереж (VPN), точкам бездротового (Wi-Fi) доступу, Ethernet комутаторів, DSL та іншим типам мережевого доступу. Завдяки відкритості, простоті впровадження, постійному удосконаленню, протокол RADIUS зараз є фактично стандартом для віддаленої аутентифікації.

Рисунок 1.7 - Аутентифікація та авторизація

Ноутбуки та IP телефон, представляють пристрої користувача, з яких необхідно виконати аутентифікації та авторизації на мережевих серверах доступу (NAS) :

- точці Wi-Fi доступу,
- маршрутизатор,
- VPN сервері і
- IP АТС.

На рисунку 1.7 показані не всі можливі варіанти NAS. Існують і інші мережеві пристрої доступу.

RADIUS протокол реалізовується у вигляді інтерфейсу між NAS, який виступає як RADIUS клієнт, і RADIUS сервером - програмним забезпеченням, яке може бути встановлено на комп'ютері (сервері) або якомусь спеціалізованому пристрої. Таким чином, RADIUS сервер, як правило, не взаємодіє безпосередньо з пристроєм користувача, а тільки через мережевий сервер доступу.

Користувач надсилає запит на мережевий сервер доступу для отримання доступу до певного мережного ресурсу, використовуючи сертифікат доступу. Сертифікат надсилається на мережевий сервер доступу через мережевий протокол канального рівня (Link Layer), наприклад, Point-to-Point Protocol (PPP) у разі виконання комутованого доступу, Digital Subscriber Line (DLS) - у разі використання відповідних модемів і т.п. NAS після цього, в свою чергу, надсилає повідомлення запиту доступу на RADIUS сервер, так званий RADIUS Access Request. Цей запит включає сертифікати доступу, які зазвичай представлені у вигляді імені користувача і пароля або сертифіката безпеки, отриманих від користувача. Крім цього запит може містити додаткові параметри, такі як мережеву адресу пристрою користувача, його телефонний номер, інформацію про фізичну адресу, з якого користувач взаємодіє з NAS.

RADIUS сервер перевіряє цю інформацію на коректність, використовуючи такі схеми аутентифікації, як PAP, CHAP, EAP і т.п. Коротко опишемо ці протоколи.

1.4 Схеми аутентифікації RADIUS сервера

PAP (Pass-word Aut-henti-cati-on Pro-tocol) (RFC1334) - простий аутентифікаційний протокол, який використовується для аутентифікації користувача по відношенню до мережевого сервера доступу (NAS). PAP використовується PPP протоколом. Практично всі сервери доступу підтримують PAP. PAP передає незашифрований пароль через мережу і, отже, є незахищеним протоколом. Тому PAP, зазвичай, використовується в тому випадку, коли сервер не підтримує захищені протоколи, такі як снаря, EAP і т.п.

CHAP (англ. Chal-lenge Hand-sha-ke Aut-henti-cati-on Pro-tocol) (RFC 1994) широко поширений алгоритм перевірки автентичності, що передбачає передачу не самого пароля користувача, а непрямих відомостей про нього. При використанні CHAP (рис. 1.8) сервер віддаленого доступу відправляє клієнту рядок запиту. На основі цього рядка і пароля користувача клієнт обчислює хеш-код MD5 (Message Digest-5) і передає його серверу.

Рисунок 1.8 - CHAP – протокол

Хеш-функція є алгоритмом одностороннього (незворотного) шифрування, оскільки значення хеш-функції для блоку даних обчислити легко, а визначити вихідний блок по хеш-коду з математичної точки зору неможливо за прийнятний час. (За хешування існує багато літератури, наприклад, можна прочитати: Хешування). Сервер, якому доступний пароль користувача, виконує ті ж самі обчислення і порівнює результат з хеш-кодом, отриманим від клієнта. У разі збігу облікові дані клієнта віддаленого доступу вважаються справжніми.

MD5 (Mes-sa-ge-Di-gest al-go-rithm 5) (RFC 1321) — широко використовувана криптографічна функція з 128 бітовим хешем. Знайдений ряд вразливостей в алгоритмі MD5 (рис. 1.9), в силу чого в США департамент US Department of Homeland Security не рекомендує використання MD5 в майбутньому, і для більшості урядових програм с 2010 США потрібно перейти на сімейство алгоритму SHA-2.

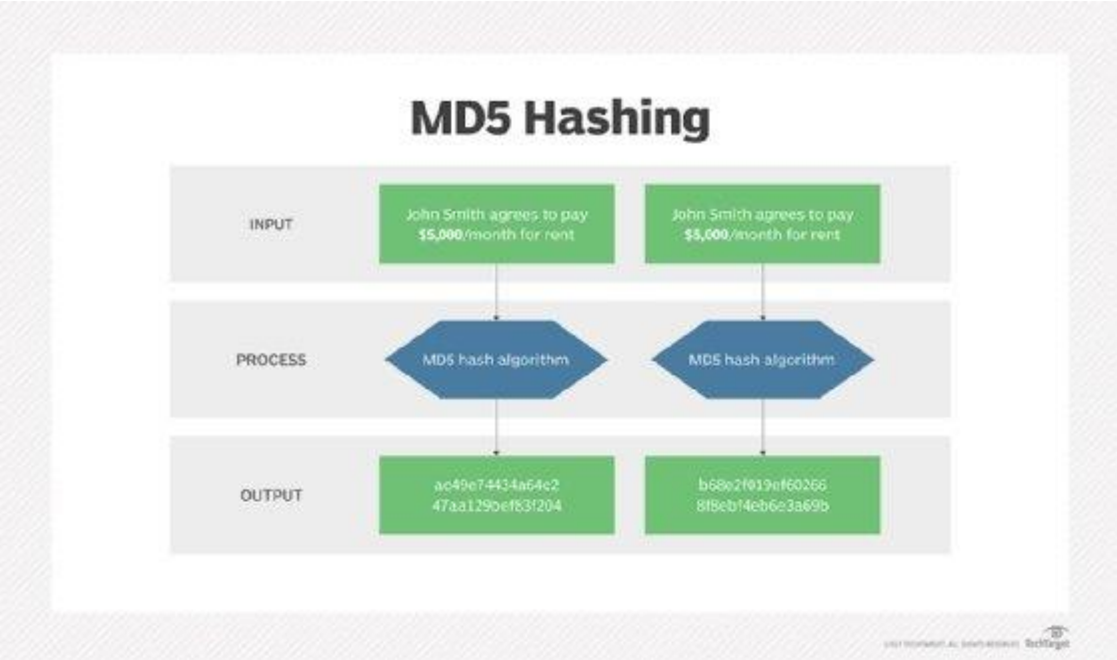


Рисунок 1.9 - MD5 (Message Digest algorithm 5)

Протокол EAP (Extensible Authentication Protocol) (RFC 3748) дозволяє перевіряти справжність при підключеннях віддаленого доступу за допомогою різних механізмів перевірки автентичності. Точна схема перевірки справжності узгоджується клієнтом віддаленого доступу і сервером, який виконує перевірку автентичності (ним може бути сервер віддаленого доступу або RADIUS сервер). За умовчанням в маршрутизацію та віддалений доступ включена підтримка протоколів EAP-TLS і MD5-Challenge (MD5-задача). Підключення інших модулів EAP до сервера, який використовує маршрутизацію та віддалений доступ, забезпечує підтримку інших методів EAP.

Рис. 2.0 - Протокол EAP

Протокол EAP (рис. 2.0) дозволяє вести вільний діалог між клієнтом віддаленого доступу і системою перевірки автентичності. Такий діалог складається із запитів системи перевірки справжності на необхідну їй інформацію і відповідей клієнта віддаленого доступу. Наприклад, коли протокол EAP використовується з генераторами кодів доступу, сервер, що виконує перевірку справжності, може окремо запитувати у клієнта віддаленого доступу ім'я користувача, ідентифікатор і код доступу. Після відповіді на кожен такий запит клієнт віддаленого доступу проходить певний рівень перевірки автентичності. Коли на всі запити будуть отримані задовільні відповіді, перевірка достовірності клієнта віддаленого доступу успішно завершується.

Схеми перевірки автентичності, що використовують протокол EAP, називаються типами EAP. Для успішної перевірки автентичності клієнт віддаленого доступу і сервер, що виконує перевірку автентичності, повинні підтримувати один і той же тип EAP.

Тепер повернемося до RADIUS сервера, який перевіряє інформацію, отриману від NAS. Сервер перевіряє ідентичність користувача, а також коректність додаткової інформації, яка може міститися в запиті: мережеву адресу пристрою користувача, телефонний номер, стан рахунку, його привілеї при доступі до запитуваного мережного ресурсу. За результатами перевірки RADIUS сервер посилає NAS один з трьох типів відгуків:

Ac-cess-Re-ject. показує, що даний користувальницький запит невірний. При бажанні сервер може включити текстове повідомлення в Access-Reject, яке може бути передано клієнтом користувачеві. Ніякі інші атрибути (крім Proxy-State) не дозволені в Access-Reject.

Ac-cess-Chal-lenge. Запит додаткової інформації від користувача, наприклад, другий пароль, пін-код, номер картки і т.п. Цей відгук також використовується для більш повного аутентификационного діалогу, де захисний тунель виконується між пристроєм користувача і RADIUS сервером, так що сертифікати доступу ховаються від NAS.

Ac-cess Ac-cept. Користувачеві дозволений доступ. Оскільки користувач аутентифікований, то RADIUS сервер перевіряє авторизацію на використання запитаних користувачем ресурсів. Наприклад, користувачеві може бути доступ через бездротову мережу, але заборонений доступ до VPN мережі.

1.5 Висновки

Під час дослідження предметної області, її структурних та функціональних особливостей було виявлено ефективність використання системи RADIUS, яка може забезпечити управління точками доступу Wi-Fi, та може контролювати доступ до цих радіоточок на основі автентифікації та авторизації користувачів.

2. МОДЕЛЮВАННЯ ТА ПРОЄКТУВАННЯ СИСТЕМИ УПРАВЛІННЯ

2.1 Моделювання та проектування системи управління

Моделювання та проектування системи управління Wi-Fi радіоспотами з використанням системи RADIUS (Remote Authentication Dial-In User Service) передбачає розробку архітектури та конфігурації всіх компонентів системи:

- Wi-Fi радіоспоти - це пристрої, які надають бездротовий доступ до Інтернету для користувачів.
- RADIUS сервер - це сервер, який використовується для автентифікації, авторизації та обліку користувачів, що підключаються до Wi-Fi радіоспотів. RADIUS дозволяє виконувати ці процеси централізовано та контролювати доступ користувачів до мережі.
- Керуючий пристрій (керуючий контролер) - це пристрій, який використовується для керування Wi-Fi радіоспотами та їх налаштування.
- Система моніторингу та аналізу мережі - це система, яка дозволяє аналізувати та моніторити пропускну здатність мережі, щоб забезпечити ефективну роботу всіх компонентів системи.

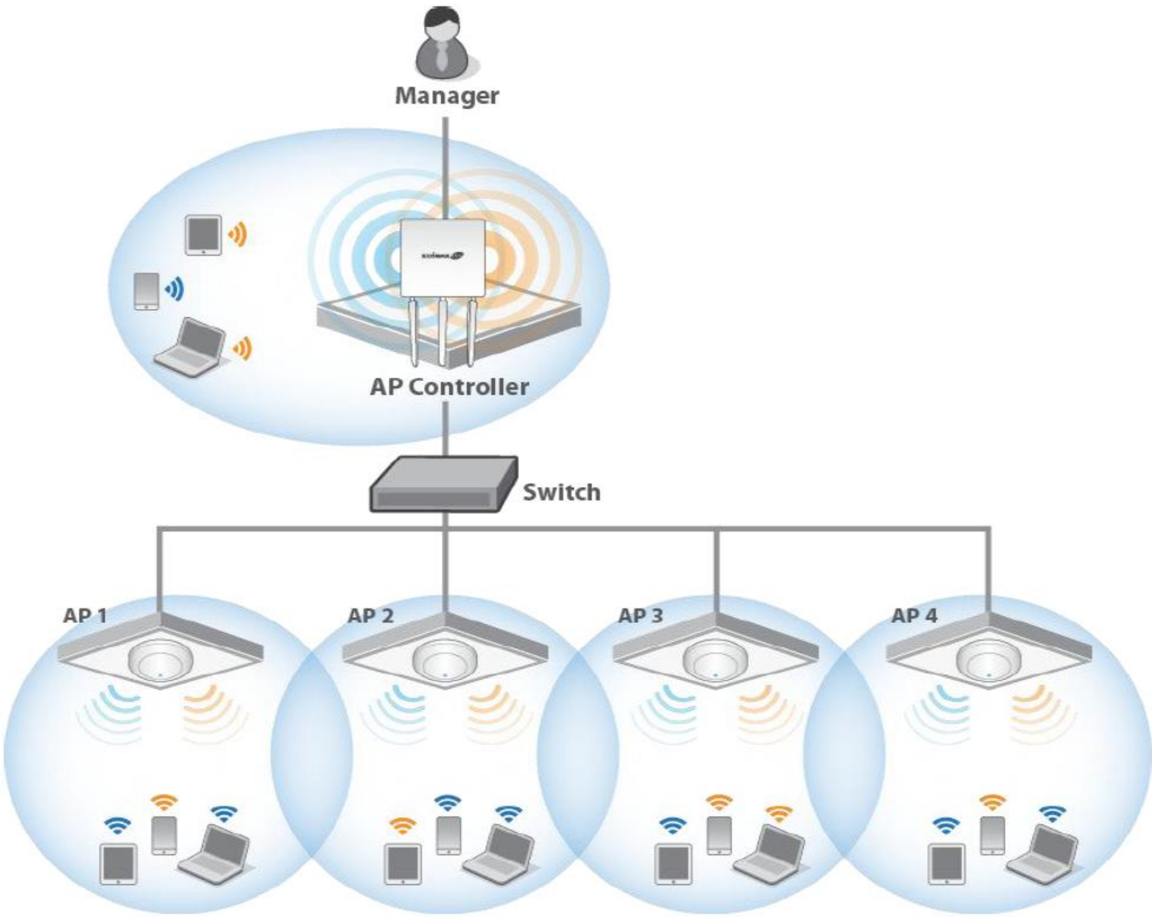


Рисунок 2.1 - вбудований RADIUS-сервер

2.2 Для проектування та моделювання такої системи необхідно виконати наступні кроки:

1. Визначити вимоги до мережі - це включає визначення кількості користувачів, об'єму трафіку, розміщення Wi-Fi радіоспотів, потреби у резервному живленні та забезпеченні безпеки мережі.

2. Вибрати Wi-Fi радіоспоти - необхідно вибрати такі радіоспоти, які задовольнять вимоги до мережі. Важливо враховувати такі параметри, як швидкість передачі даних, покриття, максимальну кількість підключених користувачів та інші.

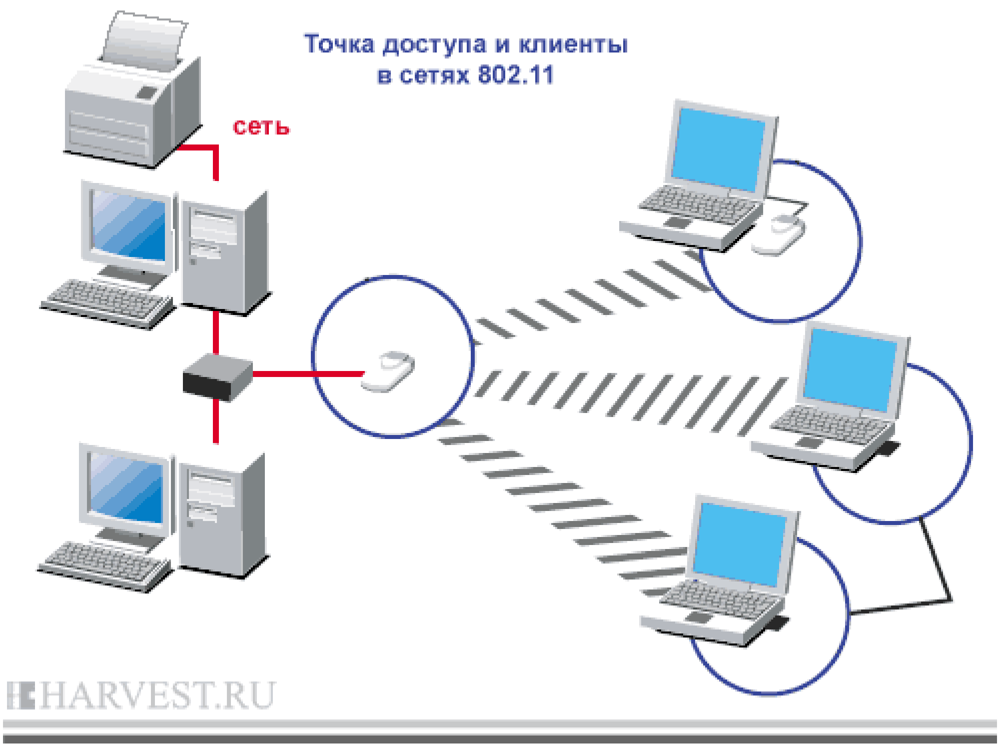


Рисунок 2.2 - кількість користувачів

3. Визначте, які сервери будуть використовуватися для розгортання системи RADIUS. Розгляньте можливості використання існуючих серверів або потребу розгортання нових.

4. Встановіть та налаштуйте сервер RADIUS на кожному сервері. Налаштуйте параметри для автентифікації та авторизації користувачів.

5. Налаштуйте мережеві пристрої (наприклад, маршрутизатори, комутатори) для використання серверів RADIUS для автентифікації та авторизації користувачів. Налаштуйте параметри доступу до мережевих ресурсів, зокрема, права доступу до файлів та директорій.

6. Перевірте, чи працює система RADIUS правильно. Спробуйте авторизуватися на мережевих пристроях з різних місць та перевірте, чи доступ до ресурсів належним чином обмежується згідно з налаштуваннями доступу.

7. Налаштуйте моніторинг та журналювання системи RADIUS (рис. 2.2), щоб забезпечити відстеження дій користувачів та виявлення проблем у системі.

Ці кроки допоможуть вам успішно розгорнути та налаштувати систему RADIUS для автентифікації та авторизації користувачів в мережі.

2.3 Список кроків для моделювання та проектування системи управління RADIUS

Продовжуючи список кроків для моделювання та проектування системи управління RADIUS, після визначення вимог до системи потрібно вибрати платформу, на якій вона буде працювати. Для вибору платформи можна враховувати наступні фактори:

Обсяг мережі: Якщо мережа велика, потрібно вибрати потужну платформу, яка може обслуговувати багато користувачів та пристроїв.

Безпека: Платформа повинна мати високий рівень безпеки для захисту від несанкціонованого доступу.

Доступність: Платформа повинна бути доступною для адміністраторів мережі для здійснення необхідних налаштувань та керування мережею.

Сумісність: Платформа повинна бути сумісною зі звичайними RADIUS-серверами та іншими пристроями в мережі такими як на (рис. 2.3)

Масштабованість: Платформа повинна бути масштабованою, щоб забезпечити майбутні потреби мережі.

Вартість: Вартість платформи може бути важливим фактором при виборі, тому потрібно враховувати бюджет проекту.

Рисунок 2.3 - сервер FreeRADIUS

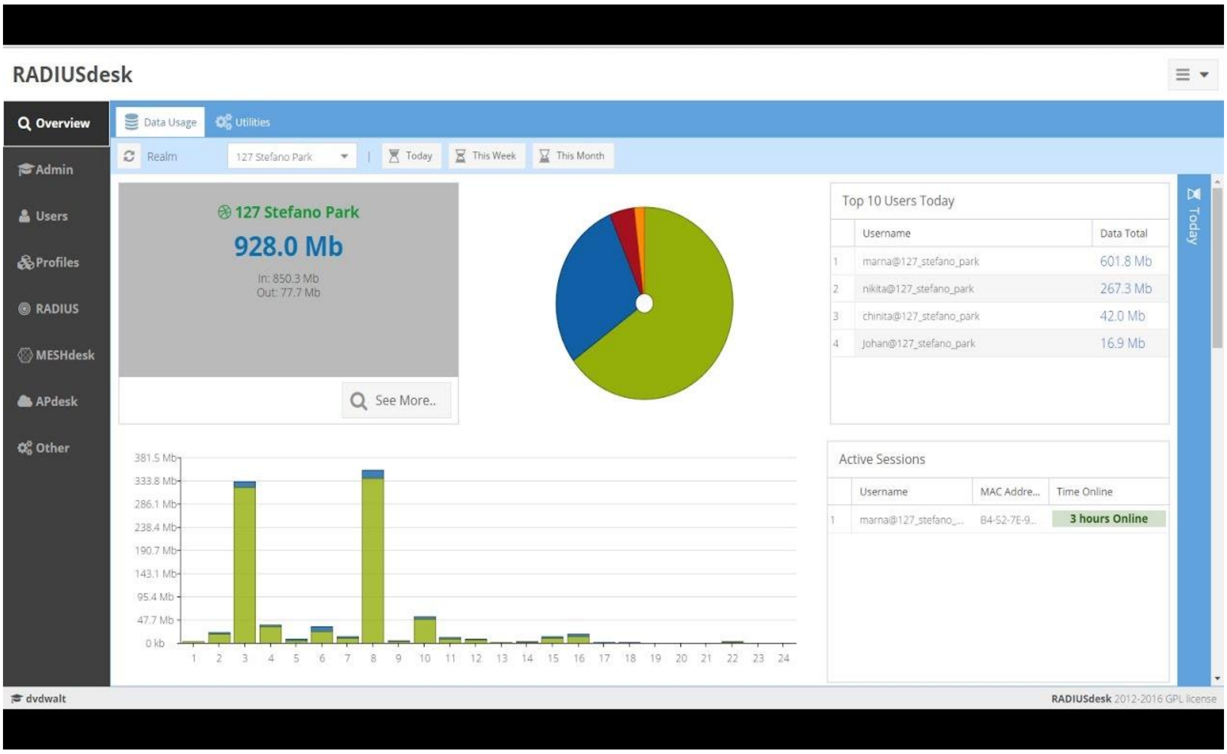


Рисунок 2.4 - програмне забезпечення FreeRADIUS

Зазвичай для системи управління RADIUS використовують сервери на базі операційних систем, таких як Windows Server або Linux (рис. 2.4), що забезпечують високу безпеку та масштабованість. Також можна розглянути використання готових рішень RADIUS-серверів, таких як FreeRADIUS або Cisco ACS.

2.4 Конфігурація WLC

Конфігурація WLC (Wireless LAN Controller) - це процес налаштування параметрів, політик та функцій на WLC для керування бездротовою мережею. WLC є централізованим пристроєм, який управляє точками доступу (AP) та забезпечує керування та координацію роботи бездротової мережі.

Основна мета конфігурації WLC - забезпечити безперебійну та надійну роботу бездротової мережі шляхом налаштування параметрів, які визначають поведінку WLC та точок доступу.

Ось кілька кроків для базової конфігурації WLC:

Підключіться до WLC: Використовуйте консольний кабель або SSH-клієнт для з'єднання з WLC.

Налаштуйте основні параметри мережі: Встановіть IP-адрес, маску підмережі та шлюз за замовчуванням на WLC. Це можна зробити через CLI або веб-інтерфейс.

Створіть WLAN (Wireless LAN): Визначте ідентифікатор WLAN, безпеку (наприклад, WPA2), SSID та інші параметри безпеки, такі як ключі шифрування. Це можна зробити через веб-інтерфейс WLC.

Налаштуйте інтерфейси мережі: Визначте інтерфейси, які будуть використовуватися для зв'язку з мережею, такі як мережеві інтерфейси, інтерфейси керування, інтерфейси моніторингу тощо. Налаштуйте їх параметри, такі як режим роботи, IP-адреси, VLAN і т. д.

Налаштуйте точки доступу (AP): Додайте точки доступу до WLC, вказавши їх ідентифікатори, інформацію про безпеку та інші налаштування. WLC автоматично налаштовує точки доступу і керує ними.

Налаштуйте параметри керування мережею: Визначте політики керування ресурсами, які включають в себе параметри, такі як керування пропускною здатністю, додаткові послуги, керування роумінгом тощо.

Збережіть і перевірте конфігурацію: Після внесення всіх необхідних змін збережіть конфігурацію WLC.

Створимо базову мережу за допомогою контролера бездротової локальної мережі Cisco (WLC) і двох точок доступу. Тут використані точки доступу Cisco WLC 2504 і 2702, але підійдуть будь-які інші WLC і точки доступу. Розглянемо, як налаштувати WLC і комутатор, графічний інтерфейс WLC.

Ця мережа матиме три VLAN: 10, 20 і 30:

-VLAN 10 - це керуюча VLAN. WLC використовує інтерфейс керування для зв'язку з точками доступу, і ми можемо використовувати інтерфейс керування для налаштування WLC через SSH або графічний інтерфейс.

-VLAN 20 і 30 призначені для бездротових мереж.

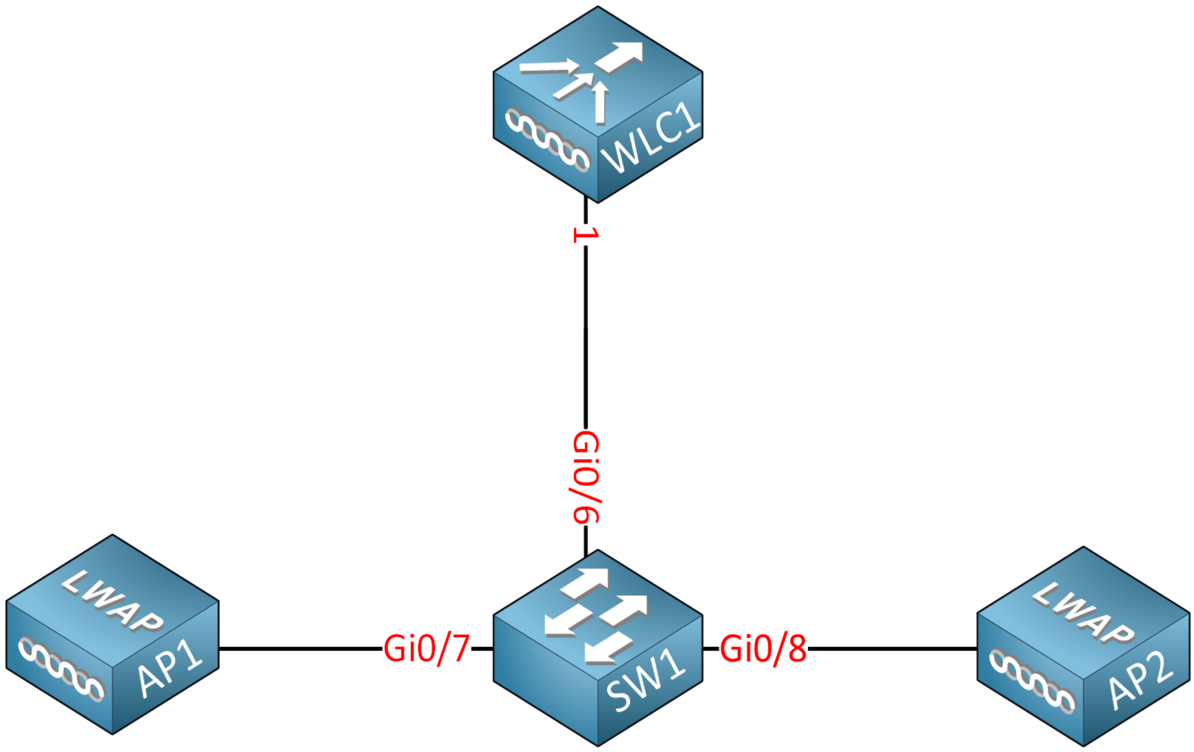


Рисунок 2.4 – Фізичний тополь

Відокремимо наш трафік керування від трафіку бездротових клієнтів, тому створимо окрему VLAN для керування. Кожен SSID можна зіставити з окремою VLAN, тому, маючи дві VLAN, можемо створити дві окремі бездротові мережі. Наприклад, можемо створити одну бездротову мережу для корпоративних користувачів, а іншу - для гостьових користувачів (рис. 2.4). Налаштуємо SW1 як DHCP-сервер, щоб точки доступу отримували динамічну IP-адресу. Точки доступу зможуть знайти WLC автоматично, оскільки вони знаходяться в одній VLAN.

1.5 VLAN (Virtual Local Area Network)

VLAN (Virtual Local Area Network) - це технологія мережевого рівня, яка дозволяє логічно розділити одну фізичну локальну мережу на кілька логічних сегментів. Кожен VLAN функціонує незалежно і може мати свої власні налаштування, правила безпеки та політики комутації. Щоб фізично копіювати функції VLAN, потрібно встановити окремий, паралельний збір мережевих кабелів і перемикачів, які зберігаються окремо від первинної мережі. Але на відміну від фізичної відділеної мережі, VLAN ділить пропускну здатність; дві окремих одно-гігабітних віртуальних мережі які використовують одно-гігабітний зв'язок мають занижену пропускну здатність. Це віртуалізує поведінку VLAN (налаштування портів комутатора, позначки кадрів при вході в мережу VLAN, пошук MAC таблиці, щоб перейти до магістральних контактів і видалення тегів при виході з VLAN). VLAN (рис. 2.5) дозволяє розділити фізичну мережу на логічні сегменти, що дозволяє керувати ізоляцією і безпекою різних груп користувачів або пристроїв. Віртуальне розділення мережі допомагає покращити продуктивність, безпеку та керованість мережевого трафіку.

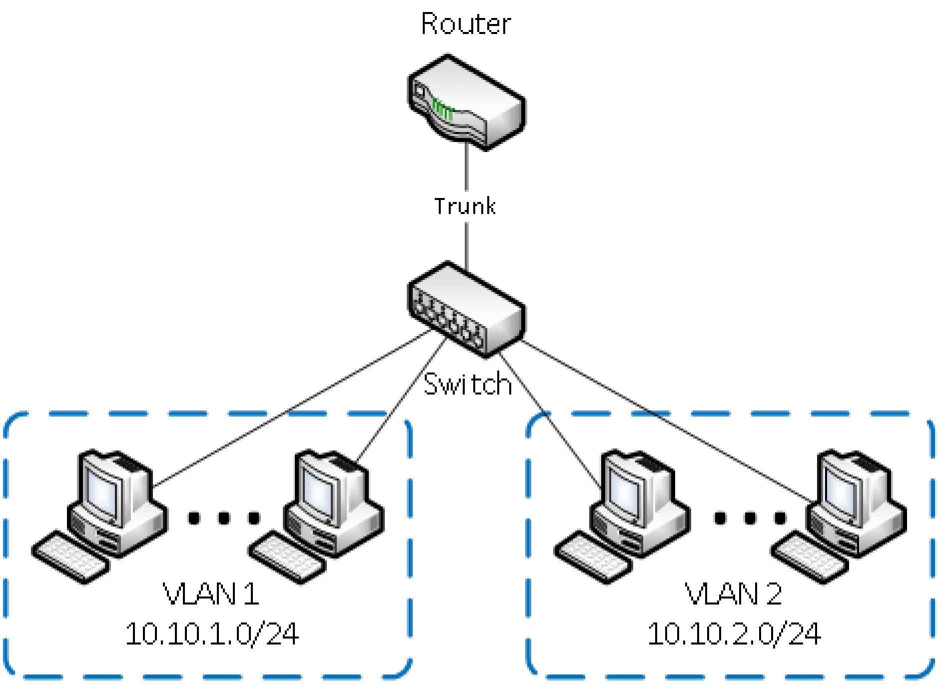


Рис. 2.5 – Конфігурація VLAN

VLAN дозволяє розділити фізичну мережу на логічні сегменти, що дозволяє керувати ізоляцією і безпекою різних груп користувачів або пристроїв. Віртуальне розділення мережі допомагає покращити продуктивність, безпеку та керованість мережевого трафіку. VLAN дозволяє розділити фізичну мережу на логічні сегменти, що дозволяє керувати ізоляцією і безпекою різних груп користувачів або пристроїв. Віртуальне розділення мережі допомагає покращити продуктивність, безпеку та керованість мережевого трафіку. Завдяки VLAN можна обмежити розповсюдження мережевого трафіку тільки на необхідні сегменти мережі. Це дозволяє зменшити навантаження на комутатори та підвищити продуктивність мережі. Використання VLAN дозволяє налаштувати різні рівні безпеки для різних сегментів мережі. Це дозволяє контролювати доступ до ресурсів та обмежувати розповсюдження шкідливого трафіку в мережі. Використання VLAN дозволяє ефективно використовувати наявне мережеве обладнання, не потребуючи фізичного розширення мережі. Ви можете логічно розділити мережу без необхідності додаткових комутаторів або кабельної інфраструктури.

Недоліки використання VLAN. Управління великою кількістю VLAN може бути складним і заплутаним завданням. Кожна VLAN потребує відповідних налаштувань на комутаторах і маршрутизаторах, а також моніторингу та керування трафіком. Це може бути складно в умовах складної мережевої інфраструктури.

Неправильна настройка або недосконала безпека VLAN може призвести до можливості вторгнення між VLAN або зловживання даними. Наприклад, атака VLAN хопінгу може дозволити зловмиснику проникнути з одного VLAN в інший.

Якщо неконтрольована кількість VLAN з'єднана на одному комутаторі, це може призвести до затримок у комутації та погіршення продуктивності. При проектуванні VLAN необхідно враховувати розмір і пропускну спроможність комутаторів. При проблемах у мережі, пов'язаних з VLAN, відлагодження може бути важким завданням. Встановлення правильного VLAN-налаштування та виявлення проблемних точок може вимагати певного рівня експертизи і часу. Великі мережі з великою кількістю VLAN можуть зазнавати обмежень в масштабованості. Маршрутизатори та комутатори можуть потребувати значних ресурсів для керування та обробки трафіку між VLAN, що може призвести до погіршення продуктивності мережі. Враховуючи ці недоліки, важливо правильно спланувати та налаштувати VLAN для досягнення оптимальної продуктивності та безпеки.

2.5 Базова конфігурація контролера бездротової локальної мережі Cisco

Розподілена архітектура WiFi: У розподіленій архітектурі всі точки доступу WiFi є автономними і називаються автономними або окремими ТД. Автономні точки доступу працюють індивідуально і повинні налаштовуватися і управлятися окремо. У цій архітектурі автономна точка доступу виконує як операції 802.11, так і операції керування.

Централізована архітектура WiFi: У централізованій архітектурі точки доступу контролюються і управляються центральним пристроєм, який називається Wireless LAN Controller (WLC), і такі точки доступу називаються полегшеними точками доступу. Полегшена точка доступу виконує тільки операції 802.11 в режимі реального часу. Всі функції управління зазвичай виконуються на контролері бездротової мережі. Полегшена точка доступу не може працювати самостійно.

Перш ніж перейти до налаштування, розглянемо порти контролера бездротової локальної мережі, інтерфейси контролера та протокол CAPWAP.

Порти контролера - це фізичні порти пристрою.

Сервісний порт (SP): використовується для початкового завантаження, відновлення системи та управління поза діапазоном. Якщо ви хочете налаштувати контролер за допомогою графічного інтерфейсу, вам потрібно підключити комп'ютер до сервісного порту.

Порт резервування (RP): Цей порт використовується для підключення іншого контролера для резервування операцій.

Порти розподілу: Ці порти використовуються для всіх точок доступу і трафіку управління. Порт розподілу підключається до порту комутатора в режимі магістралі. Контролери серії 4400 мають чотири порти розподілу, а контролери серії 5500 - вісім портів розподілу.

Порт консолі: Використовується для позасмугового керування, відновлення системи та початкового завантаження.

2.6 CAPWAP (Control and Provisioning of Wireless Access Points)

CAPWAP (Control and Provisioning of Wireless Access Points) - це протокол, який дозволяє зв'язати легку точку доступу з бездротовою локальною мережею (WLC). Протокол CAPWAP інкапсулює трафік між легкою точкою доступу і WLC у віртуальний тунель, який називається тунель CAPWAP. Весь трафік від точки доступу до WLC проходить через цей тунель. Тому слід мати на увазі, що в централізованій архітектурі WiFi весь трафік від точок доступу закінчується на контролері WLC, а потім перенаправляється з контролера в дротову мережу.

Базова конфігурація Cisco WLC - Для доступу до інтерфейсу командної строки потрібно підключити комп'ютер до консольного порту контролера бездротової локальної мережі за допомогою консольного кабелю.

CAPWAP базується на полегшеному протоколі точки доступу (LWAPP). Машина станів CAPWAP (рис. 2.5) схожа на LWAPP, але з додаванням повного встановлення тунелю Datagram Transport Layer Security (DTLS). Стандарт забезпечує управління конфігурацією і управління пристроями, дозволяючи передавати конфігурації і вбудоване програмне забезпечення до точок доступу (AP). Оскільки загальна структура стану протоколу CAPWAP в основному така ж, як у кінцевого автомата (FSM) в LWAPP, детальна діаграма не потрібна. Протокол використовує загальний механізм інкапсуляції та транспортування, що робить його незалежним від конкретної радіотехнології.

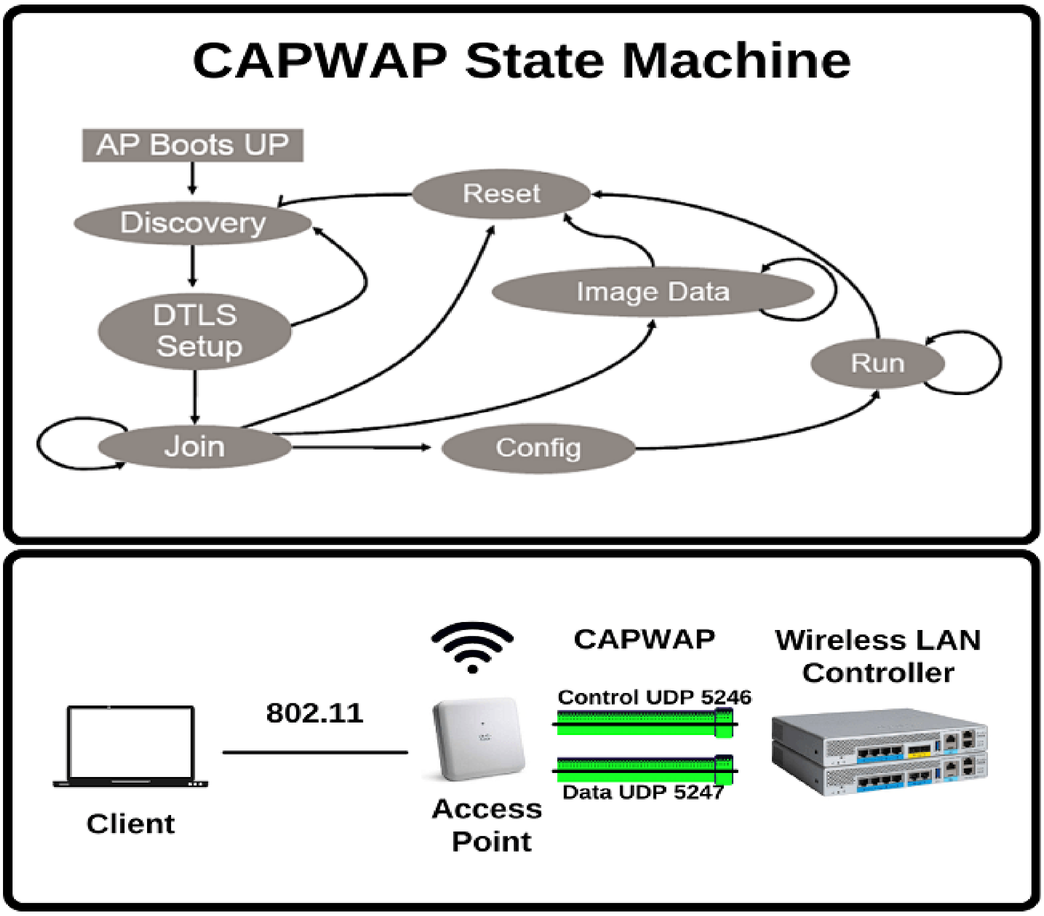


Рисунок 2.5 - Протокол CAPWAP

Специфікація CAPWAP для конкретної бездротової технології називається прив'язкою. Прив'язка до IEEE 802.11 описана в RFC 5416. Коли CAPWAP підтримується і ввімкнена, першою функцією є ініціювання фази виявлення. Бездротові точки доступу шукають контролер, надсилаючи повідомлення із запитом на виявлення. Після отримання запиту на виявлення контролер відповідає відповіддю на виявлення.

На цьому етапі два пристрої встановлюють безпечне з'єднання за допомогою протоколу Datagram Transport Layer Security для обміну керуючими повідомленнями CAPWAP і повідомленнями даних. Керуючі повідомлення містять інформацію та інструкції, пов'язані з управлінням бездротовою локальною мережею (WLAN). Повідомлення даних інкапсулюють переслані бездротові кадри. Кожне з них надсилається через окремий порт протоколу дейтаграм користувача. У режимі розділеного MAC протокол CAPWAP інкапсулює всі бездротові кадри даних і керування 2-го рівня, які потім обмінюються між контролером і точкою доступу. Локальний режим MAC-адреси дозволяє локально мостити або тунелювати кадри даних як кадри Інтернет. В обох режимах точка доступу локально обробляє кадри керування бездротового зв'язку 2-го рівня, а потім пересилає їх на контролер.

Протокол також був розроблений для підтримки функціональної сумісності в мультивендорних WLAN. Але більшість розробників, які його реалізували, додали власні розширення, якими забороняють сумісність.

2.7 Розробка концептуальної моделі системи RADIUS за допомогою ER-діаграми

ER-діаграма - це графічне зображення сутностей та їх зв'язків, що використовується для моделювання концептуальної моделі даних.

При розробці концептуальної моделі системи управління RADIUS за допомогою ER-діаграми (рис. 2.6), перш за все, потрібно визначити сутності та зв'язки між ними. Наприклад, можна виділити наступні сутності:

Користувач: містить інформацію про ідентифікацію та авторизацію користувачів, таку як ім'я, пароль, IP-адресу тощо.

Клієнт: містить інформацію про клієнтів, що використовують систему RADIUS, таку як ідентифікатор, пароль, IP-адресу тощо.

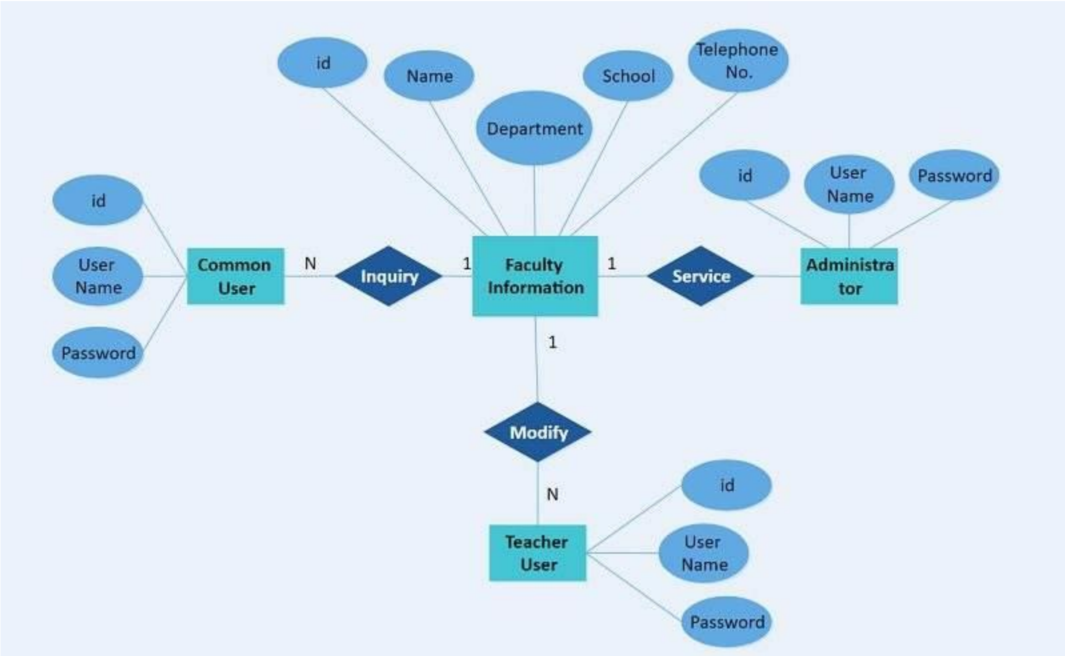


Рисунок 2.6 - ER-діаграма

Сервер: містить інформацію про сервери, що використовують систему RADIUS, таку як IP-адресу, порт, пароль тощо.

Запис у журналі: містить інформацію про кожну авторизацію користувача, яка пройшла через систему RADIUS.

Налаштування: містить настройки та параметри системи RADIUS.

Після визначення сутностей можна визначити зв'язки між ними. Наприклад, можна визначити наступні зв'язки:

Користувач має зв'язок з клієнтом, оскільки один користувач може використовувати різних клієнтів.

Клієнт має зв'язок з сервером, оскільки клієнт може використовувати різні сервери.

Сервер має зв'язок з користувачем, оскільки на сервері можуть авторизуватись різні користувачі.

Запис у журналі має зв'язок з користувачем та клієнтом, оскільки кожен запис містить інформацію про конкретного користувача.

2.8 Тестування системи RADIUS

Це процес перевірки функціональності та коректності роботи системи управління доступом користувачів до мережевих ресурсів.

Основні етапи тестування системи RADIUS:

Підготовка тестового середовища: налаштування тестового середовища, створення тестових облікових записів, клієнтів та серверів.

Виконання базових тестів: перевірка з'єднання з RADIUS-сервером, авторизації користувача, перевірка журналу подій та настройки RADIUS-сервера.

Виконання функціональних тестів: перевірка роботи RADIUS-сервера під час зміни паролю користувача, блокування користувача, перевірка роботи з криптографічними алгоритмами тощо.

Виконання навантажувальних тестів: перевірка роботи системи RADIUS при високому навантаженні.

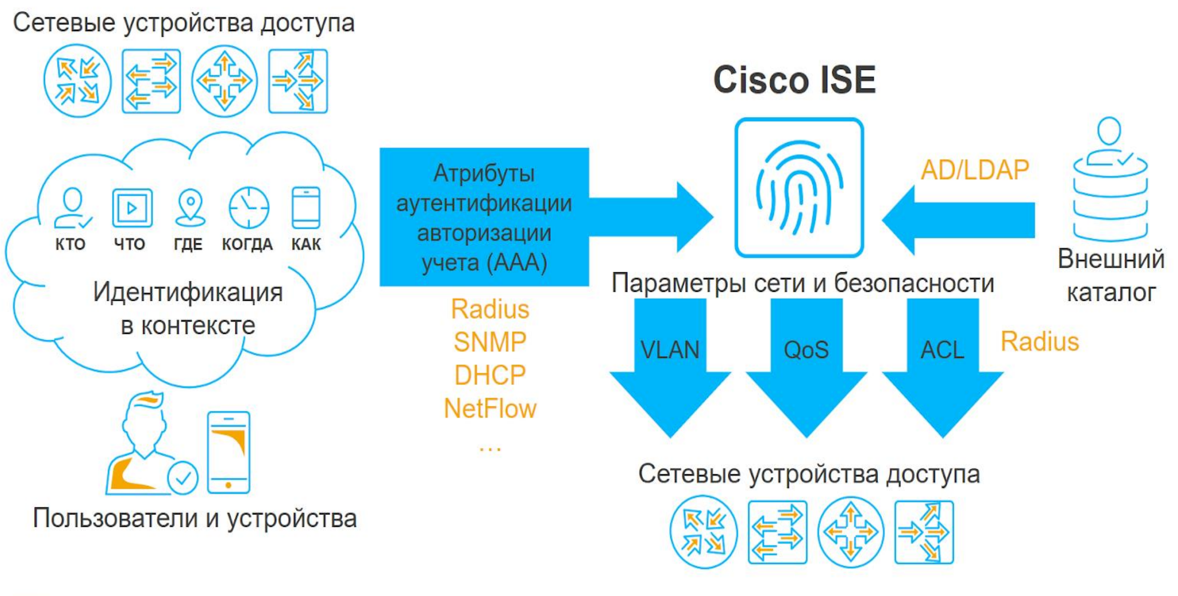


Рисунок 2.7 - побудова ER-діаграми

Тестування безпеки: перевірка захисту системи RADIUS від зловмисників, перевірка роботи механізмів аутентифікації та авторизації.

Після завершення тестування необхідно проаналізувати результати тестів та визначити проблеми, які були виявлені. Після виявлення проблем необхідно внести зміни в систему та повторити тестування. Після успішного завершення тестування можна переходити до етапу впровадження системи RADIUS в роботу.

2.9 Чому варто використовувати RADIUS Server?

Централізована система автентифікації : всі запити користувачів на доступ і автентифікацію обробляються з однієї точки незалежно від різних конфігурацій пристрою.

Поліпшена мережна безпека. Наявність централізованого управління автентифікацією та авторизацією підвищує безпеку мережі та заощаджує час та зусилля. Користувачі мають власні облікові дані для доступу до мереж Wi-Fi. Якщо мережний комутатор або бездротовий маршрутизатор підтримує автентифікацію RADIUS, можна настроїти RADIUS Server на Synology Router для автентифікації доступу Wi-Fi для облікових записів локальної системи, домену або LDAP.

Хоча традиційна служба автентифікації має свої переваги, хмарна автентифікація RADIUS надає всі переваги без клопоту з підтримкою локальної інфраструктури для автентифікації RADIUS. Сьогодні одним з найкращих рішень RADIUS є RADIUS у хмарі. Функція хмарного RADIUS від JumpCloud забезпечує додаткову безпеку, таку як складність пароля, MFA та динамічне призначення VLAN, без складної конфігурації та стресу під час початкового налаштування.

Налаштування RADIUS Server

1. Перейдіть до розділу RADIUS Server > Установки. За замовчуванням використовується порт автентифікації 1812, а для рівня профілю SSL/TLS встановлено значення Проміжна сумісність .

2 .Виберіть одне з наведених нижче облікових записів для автентифікації за допомогою RADIUS Server.

Локальні користувачі : локальні облікові записи, налаштовані в SRM , будуть перевірені.

Користувачі LDAP: Synology Router необхідно налаштувати як клієнт LDAP.

Користувачі домену: Synology Router необхідно налаштувати як клієнт домену.

3. Щоб додати клієнтів, перейдіть до розділу RADIUS Server > Клієнти

Клієнти - це пристрої, наприклад мережні комутатори, бездротові маршрутизатори або сервери VPN, яким можна запитувати автентифікацію та авторизацію RADIUS Server.

Документацію до мережного пристрою для отримання інформації про налаштування клієнта для використання RADIUS Server.

Як правило, вам знадобиться така інформація:

1. IP-адреса: введіть локальну IP-адресу Synology Router.

2. Номер порту: введіть порт, який використовується RADIUS Server.

3. Загальний секрет: введіть загальний секрет, налаштований у RADIUS Server.

Ви також можете налаштувати бездротову мережу WPA2-Enterprise за допомогою RADIUS Server.

2.10 Недоліки у ваикористанні RADIUS server

Хоча radius-сервери є дуже корисними і популярними в сфері мережевої безпеки, вони також можуть мати деякі недоліки.

Складність налаштування: Налаштування radius-сервера може бути складним завданням, особливо для новачків у цій області. Є багато параметрів та конфігураційних опцій, які потрібно враховувати, що може вимагати досить глибоких знань мережевої інфраструктури.

У деяких випадках radius-сервери можуть мати обмежену масштабованість, особливо при великій кількості одночасних запитів. Це може призвести до затримок у відповідях сервера та незадовільної продуктивності.

Небезпека однотипних атак: Якщо radius-сервер не налаштований або не захищений належним чином, це може зробити його вразливим до різних видів атак, таких як перехоплення інформації або перебір паролів. Це може призвести до компрометації безпеки мережі та витоку конфіденційних даних.

Складнощі у встановленні та підтримці: Встановлення та налагодження radius-сервера можуть бути складними завданнями для некваліфікованих адміністраторів мережі. Крім того, підтримка сервера та вирішення проблем, які виникають під час його роботи, також можуть бути вимогливими з точки зору знань та досвіду.

Обслуговування локального обладнання може бути складним і трудомістким. Регулярне обслуговування і моніторинг означають, що з часом управління локальними серверами може стати більш інтенсивним і неприємним.

Початкове налаштування не-хостингового RADIUS-сервера: IT-адміністраторам також може бути складно впровадити та інтегрувати в існуючий IT-ландшафт, особливо якщо організація вже підтримує локальні застарілі служби, такі як Active Directory.

Уразливості безпеки при неправильному впровадженні: Як і будь-яка інша технологія, автентифікація RADIUS може створити нові загрози безпеці організації, якщо її впровадити неправильно. На щастя, при використанні хостингу RADIUS основна частина налаштувань виконується автоматично , що дозволяє менше турбуватися про безпеку.

Широкий вибір варіантів конфігурації: На серверах RADIUS конфігурація і початкове налаштування можуть бути складними і лякаючими через широкий спектр протоколів і проблем сумісності. Навіть найдосвідченішим IT-адміністраторам доводиться проходити через складний процес конфігурації.

Коли справа доходить до програмного забезпечення сервера RADIUS і моделей реалізації, може бути важко зрозуміти, яка з них підходить саме вам. Деякі варіанти можуть бути дорогими і вимагати довгострокових зобов'язань, в той час як інші є безкоштовними, а деякі вимагають багато часу і зусиль для впровадження.

Потік інформації може бути приголомшливим і ускладнювати вибір правильного сервісу.

2.11 A. Налаштування RADIUS Server

У розділі RADIUS Server > Параметри за замовчуванням (рис. 2.8) використовується порт автентифікації 1812. Тут можна залишити його без змін.

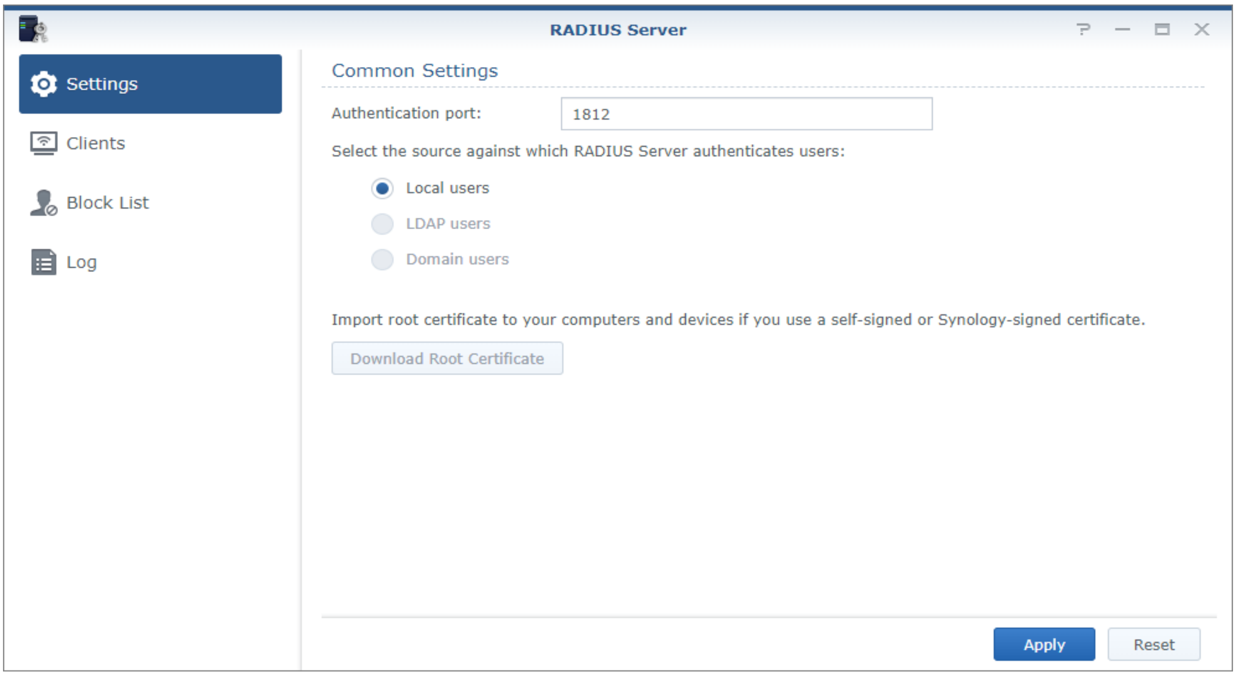


Рисунок 2.8 - Налаштування RADIUS Server

2. Перейдіть на сторінку Клієнти. Натисніть Додати та у спливаючому вікні введіть такі дані(рис. 2.9)

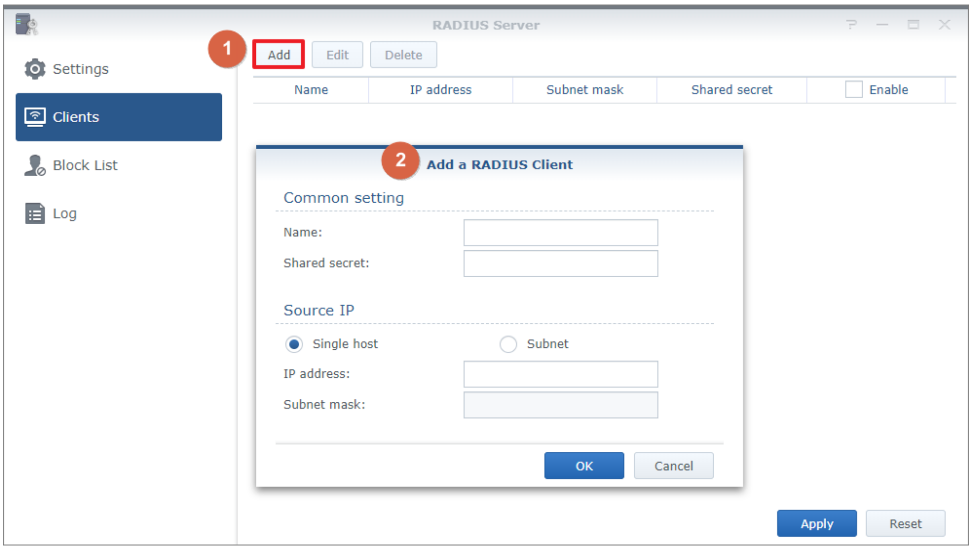


Рисунок 2.9 - Налаштування RADIUS Server

1. Ім'я. Введіть ім'я для визначення клієнта RADIUS.

2. Загальний секрет: введіть текстовий рядок загального секрету, який буде використовуватись між RADIUS Server та Synology Router.

3. IP-адреса: введіть локальну IP-адресу Synology Router.

4. Натисніть Застосувати , щоб зберегти налаштування.

Б. Керування користувачами на панелі керування.

1. Панель керування «Користувач» , створіть облікові записи користувачів, яким потрібно дозволити доступ до бездротової мережі.

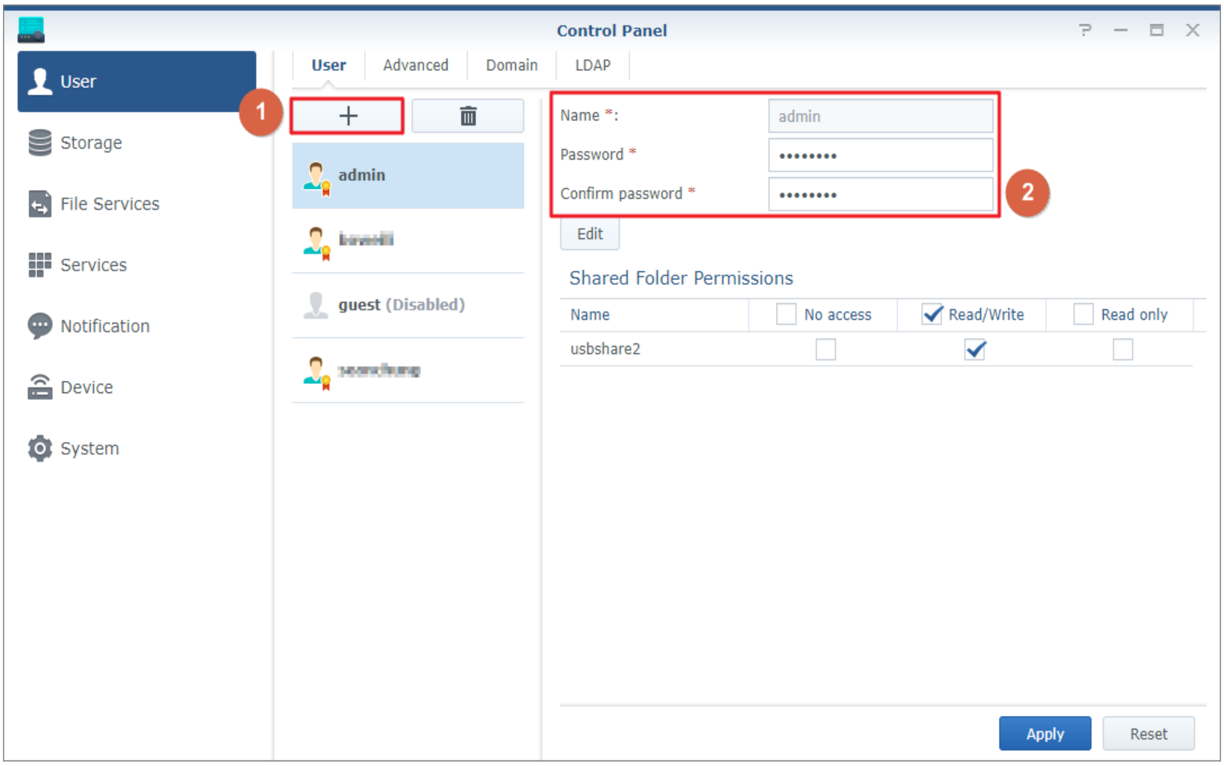


Рисунок 2.10 - Налаштування RADIUS Server

2. Натисніть Застосувати , щоб зберегти налаштування (рис. 2.10).

B. Налаштування параметрів бездротової мережі у Wi-Fi Connect

1. Перейдіть до розділу Wi-Fi Connect > Установки Wi-Fi > Мережа Wi-Fi .

2. Натисніть ... > Редагувати у верхньому правому куті цільової локальної мережі.

3. Налаштуйте такі параметри (рис. 2.11):

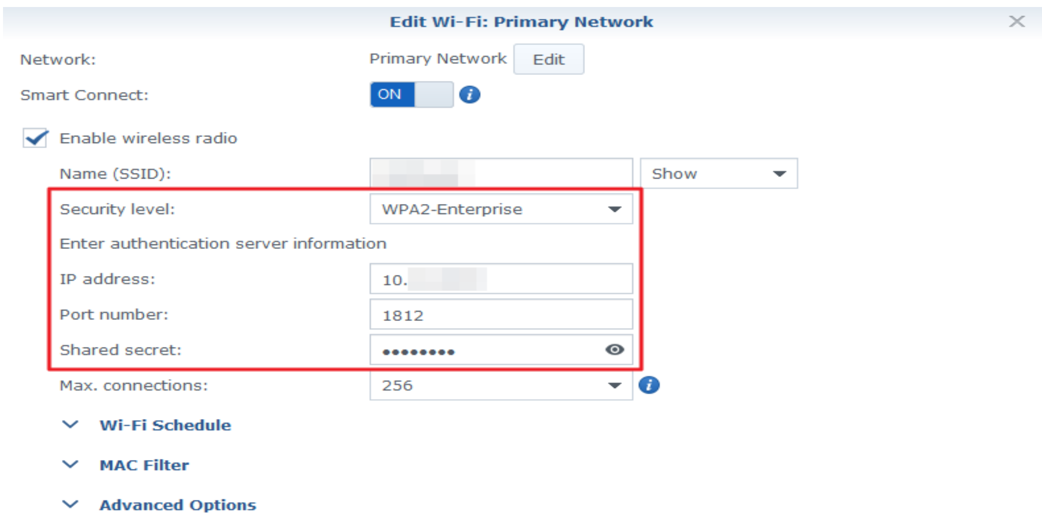


Рисунок 2.11 - Налаштування RADIUS Server

Рівень безпеки: виберіть WPA2-Enterprise. Після цього відобразяться настройки, наведені нижче.

IP-адреса: введіть IP-адресу RADIUS Server. Оскільки RADIUS Server налаштовано локально на Synology Router, введіть тут локальну IP-адресу Synology Router .

Номер порту: введіть порт, який використовується RADIUS Server.

Загальний секрет: введіть загальний секрет, налаштований у RADIUS Server.

4. Натисніть Застосувати, щоб зберегти налаштування

5. Тепер ваші клієнтські пристрої можуть підключатися до бездротової мережі WPA2-Enterprise за допомогою облікових даних.

Рисунок 2.12 - Налаштування RADIUS Server

2.12 Висновки

Відтворили модель та спроектували систему управляння Wi-Fi радіоспотами з використанням системи RADIUS (рис 2.12) разом із архітектурою та конфігураціями всіх компонентів системи. Детально розібрано кроки моделювання системи, розглянуто переваги та недоліки даної системи управління. Розглянуто покрокове налаштування RADIUS Server. Проведено і розглянуто тестування системи, застосовано базові конфігурації локальної мережі Cisco.

3. АПАРАТНА РЕАЛІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ

3.1 Радіоспоти – звичайні вайфай-роутери та їх специфікації.

Радіоспоти - це пристрої, які надають доступ до Інтернету через бездротову мережу (Wi-Fi) (рис. 3.1). Вони є сортуванням вайфай-роутерів і мають спеціальну функцію - можливість створювати бездротову точку доступу до Інтернету. Основна їх задача - розподіл інтернет-підключення з одного джерела на кілька пристроїв одночасно. Специфікації радіоспотів можуть варіюватися залежно від моделі та виробника. Основні характеристики, на які варто звернути увагу, включають стандарти бездротового зв'язку: Радіоспоти підтримують різні стандарти бездротового зв'язку, такі як 802.11ac, 802.11n, 802.11g, 802.11b. Це впливає на швидкість передачі даних і сумісність зі старішими пристроями.

Рис. 3.1 – звичайний Wi-Fi роутер

Швидкість передачі даних: Важлива характеристика, яка вказує на максимальну швидкість передачі даних через Wi-Fi. Наприклад, 300 Мбіт/с, 600 Мбіт/с, 1 Гбіт/с і т.д.

Діапазон частот: Бездротові точки доступу можуть працювати в різних діапазонах частот, таких як 2,4 ГГц і/або 5 ГГц. Діапазон 5 ГГц зазвичай забезпечує кращу швидкість і меншу перешкодження, але має менший радіус покриття, ніж діапазон 2,4 ГГц.

Кількість одночасних підключень: Радіоспоти можуть мати обмеження на кількість одночасно підключених пристроїв. Наприклад, 10, 20, 50 або більше одночасних підключень.

3.2 Основні характеристики

Швидкість підключення - перше, на що звертає увагу покупець, хоча це дуже оманливий параметр. Теоретична максимальна швидкість навіть самих недорогих сучасних роутерів становить 150 Мбіт/с (мегабіт в секунду), в той же час мало хто з провайдерів може надати реальних хоча б 100 Мбіт/с (а реально це зазвичай 10-40 Мбіт/с), тому стає зрозуміло, що приваблива фраза "до 1300 Мбіт/с" (802.11ac) в практичних умовах означає те, що реально при роботі в Інтернеті різниці з дешевими роутерами не буде ніякої. Ще один маркетинговий хід - швидкість передачі WI-FI роутера на упаковці це сума швидкостей віддачі і прийому. Тобто якщо написано WI-FI 150 Мбіт/с це означає що максимальна швидкість заванатаження буде 75 Мбіт/с і відвантаження теж 75 Мбіт/с. На швидкість передачі WI-FI сигналу негативно впливають сусідські WI-FI роутери.

Радіус дії - здавалося б, все просто, адже зазвичай вказують відстань поза і всередині приміщень, все ясно і зрозуміло. Але ці значення дуже відносні, особливо всередині приміщень, так як парочка хороших залізобетонних стін зведе нанівець сигнал навіть найпотужнішого роутера, тому по-справжньому важливими є дві наступних характеристики.

Потужність передавача - його назва говорить сама за себе і він дійсно важливий. Більшість бюджетних роутерів мають потужність передавача близько 17 дБм або навіть менше, чого зазвичай досить для того, щоб більш-менш впевнено "пробити" лише 2 стіни. Максимальна потужність, дозволена законодавством більшості країн для діапазону 2.4 ГГц, дорівнює 20 дБм (100 мВт) - вони і рекомендуються до покупки. Варто мати на увазі, що деякі Wi-Fi-роутери мають технічну можливість працювати на набагато більшій потужності, зазвичай до 27 дБм (500 мВт), тому вони відповідно до місцевого законодавства штучно знижують свою потужність.

Коефіцієнт підсилення антени вводить багатьох користувачів в оману, так як в дійсності самі антени - це пасивні пристрої і нічого самі не підилюють, вони тільки можуть вужче направляти сигнал. Наприклад, чим вище коефіцієнт підсилення всеспрямовані антени, тим більше енергії передавача йде в сторони, перпендикулярні осі антени, і тим менше енергії передавача йде вгору і вниз. Таким чином, більш потужна антена не є універсальним рішенням, так як дає можливість набагато далі "пробити" сигнал в сторони, але при цьому "забираючи" його зверху і знизу.

Кількість і тип антен. При використанні декількох антен їх енергія не підсумовується, тому це не дозволить "пробити" більшу кількість стін, а тільки зробить зв'язок більш стабільним. Різниця в якості покриття роутерами на одній антені і двох антенах значна, а от різниця між дво- і триантенними пристроями майже відсутня, останні зручно використовувати лише тоді, коли сигнал необхідно передати також і між поверхами. Щоб покрити якомога більший простір одноповерхового будинку або квартири, необхідно встановлювати антени вертикально або під невеликим кутом одна відносно іншої.

Вбудовані антени мають слабкий коефіцієнт підсилення, тому поширюють сигнал майже рівномірно на всі боки і можуть бути корисні виключно в невеликих приміщеннях або для доступу до мережі з сусідніх поверхів. Для стабільного сигналу в одноповерховому будинку або квартирі рекомендується купувати Wi-Fi-роутери на 2 антени з коефіцієнтом підсилення не менше 5 дБі.

Стабільність роботи і прошивка. Програмісти - звичайні люди і можуть помилятися, а всі їхні помилки здатні виявити тільки користувачі вже в процесі роботи. Тому на кожен роутер постійно випускаються оновлення програмного забезпечення (firmware, прошивки), які зазвичай виправляють недоліки і іноді розширюють функціональність. Щоб не потрапити на нестабільно працюючу "сиру" прошивку, рекомендується не купувати найновіші, дуже рідкісні або ексклюзивні моделі роутерів. Імовірність того, що в масовій моделі, яка випускається вже більше року, є фатальні помилки, прямує до нуля.

Дизайн. Останнє, на що необхідно звертати увагу, так як він важливий лише в офісах і навіть дуже часто красиві зовні моделі мають всеспрямовані антени вбудованого типу, які в принципі не можуть бути дуже хорошими.

3.3 Види за призначенням

Тут ми тільки виділимо основні види маршрутизаторів за призначенням.

Для квартири. Бюджет на пристрій розраховують залежно від кількості кімнат і підключених приладів. Для одно-двокімнатної квартири вистачить бюджетного роутера. Враховують рівень завантаженості ефіру: в багатоквартирних будинках у більшості є роутери, і вони перекривають один одному частоти. Через це падає швидкість, губляться пакети даних. Оптимальний варіант маршрутизатора (рис. 3.2) для квартири: дводіапазонний роутер, який вирішує проблему з частотами. Для приватного будинку. У будинках товсті стіни, які зроблені зі «складних» для радіосигналу матеріалів. Причому нормальне покриття потрібно створити не тільки для самого приміщення, а й для вулиці із зоною відпочинку. Роутери для великих різнорівневих будинків добре працюють лише з використанням репітерів. Оптимальний варіант: маршрутизатор з прошивкою, яка дозволяє створювати Mesh системи.

Рисунок 3.2 – Різновиди Wi-Fi роутерів

Для дачі/сільської місцевості. Вимоги такі ж, як у роутерів для будинку. Основна відмінність між ними у джерелі інтернету: бажано, щоб маршрутизатор міг працювати від модему або SIM-карти. Якщо ви постійно живете в сільській місцевості, то для хорошого інтернету може знадобитися спрямована антена для підключення до найближчої мобільної вишки.

Для розумного будинку. Тут великі вимоги до апаратної і програмної частини. Вимоги до начинки виходять із того, що Wi-Fi для розумного будинку повинен підтримувати мережу з великої кількості пристроїв. Не зайвим буде резервний доступ до інтернету: від двох різних провайдерів або від кабелю і модему, щоб завжди був віддалений доступ до управління будинком. Обов'язковий застосунок для смартфона, а також сумісність з гаджетами розумного будинку.

Роутери для бізнес-сегменту можна розділити на 2 групи:

1. Для офісу.

2. Для громадського простору (HoReCa, ТРЦ, виставкові майданчики, парки, інше).

Бездротовий інтернет для бізнесу рідко створюється одним роутером. Як правило, надається пакетне рішення, яке включає в себе різне устаткування, встановлення та налаштування програмного забезпечення. Це не означає, що самостійно не можна створити мережу для офісу, але часто для цього потрібен системний адміністратор.

Для офісу може знадобитися мережевий комутатор (світч), кілька точок доступу (роутерів або ретрансляторів), щоб покриття вистачало на велике приміщення. Для безпеки локальної мережі потрібен фаєрвол, а для бездротової – захисне ПЗ.

У громадських місцях швидкість менш важлива, адже Wi-Fi – це одна з додаткових опцій кафе чи бару, а не основна послуга. Тут не потрібна складна комутація, а вистачає декількох точок доступу, які просто встановити без особливих знань. Зате важливим моментом залишається безпека: ви вільно даєте підключатися до мережі сотням людей, і важливо обмежити їм доступ до налаштувань. Інакше зловмисники можуть зламати Wi-Fi, щоб заволодіти особистими даними відвідувачів, що не піде на користь вашій репутації.

Хоч для кафе вистачить швидкості до 100 Мбіт/с, з чим впорається недорогий роутер 2.4 ГГц, краще купити модель з підтримкою 5 ГГц. Причина цього – багатоканальність. На діапазоні 5 ГГц маршрутизатор без проблем одночасно працює з десятками, а то й сотнями пристроїв. Також цьому допоможе більший обсяг оперативної пам'яті: від 128 МБ.

Рисунок 3.3 – Бездротовий інтернет для бізнесу

На які характеристики звернути увагу при виборі?

Зовні роутери майже не міняються з часу появи, але стандарти Wi-Fi постійно змінюються. Наприклад, в лютому 2021 року було затверджено для використання стандарт Wi-Fi 6 (802.11ax), який потенційно може забезпечувати швидкість до 11 Гбіт/с. Тому незабаром у продажу очікуються потужні роутери, які будуть підтримувати частоту 6 ГГц (стандарт Wi-Fi 6E). Представили загалу їх ще в січні 2020 року, але поки технологія перебуає на стадії тестування.

Сьогодні на ринку присутнє обладнання, яке підтримує 6 стандартів Wi-Fi 802.11 a/b/g/n/ac/ax (розташовані в порядку поліпшення). Причому перші три стандарти (a/b/g) вже застаріли. З 2018 року для стандартів з'явилися більш зрозумілі позначення:

Wi-Fi 4 – 802.11n;

Wi-Fi 5 – 802.11ac;

Wi-Fi 6 – 802.11ax.

Площа покриття Wi-Fi на відкритому просторі залежить від потужності передавача і коефіцієнта посилення антен. Але в більшості приміщень є багато перешкод, які також впливають на дальність проходження радіохвиль.

Максимальна потужність передавача не може перевищувати 20 дБм через законодавчі обмеження. На такому рівні вона і знаходиться у більшості виробників, а для збільшення дальності мережі використовуються антени.

Варто пам'ятати про конфлікт потужності передачі і швидкості, оскільки сильний сигнал в закритому приміщенні буде відбиватися від поверхонь, що точно створить шум в мережі. Деякі виробники навіть дають можливість знизити потужність передавача в налаштуваннях роутера.

Недостатнє покриття не завжди залежить від рівня сигналу. Так, роутер може «добивати» на достатню відстань, але пристрій-клієнт не побачить мережі. Це пов'язано з високою чутливістю приймача самого клієнта, а не від площі покриття маршрутизатора. Якщо ви регулярно оновлюєте пристрої, то з такою проблемою не зіткнетеся.

Щоб врахувати цей фактор, покриття роутера коректніше відображає показник RSSI – рівень сигналу, який вимірюється в -дБм. Він не вказується виробником, оскільки залежить від різних факторів. Перевірити його можна за допомогою програми Wifi Analyzer, яку встановлюють на смартфон або планшет. Використовуючи застосунок, ви зможете вибрати краще положення для роутера, що дозволить покрити бездротовим інтернетом максимальну площу квартири або офісу.

Хорошим сигналом є показник до -65 дБм, задовільним – до -75 дБм. Якщо десь RSSI падає нижче -75, то інтернет в цьому місці буде працювати погано. Якщо виправити це переміщенням маршрутизатора не виходить, єдине рішення – використовувати репітер (ретранслятор).

3.4 Mesh системи

Рисунок 3.4 - Wi-Fi Mesh система

Роутер і ретранслятори об'єднуються в одну безшовну мережу – Wi-Fi Mesh систему (рис. 3.4). Її особливість у тому, що ви не помічаєте, як перемикаєтесь між точками доступу, адже вони створюють мережу з одним ім'ям. Тобто, коли ви підключені до маршрутизатора і поступово від нього віддаляється, то він «передасть» вас до репітера, і це не вплине на швидкість і стабільність мережі.

У ролі ретранслятора використовують окремі точки доступу або інші роутери, якщо вони підтримують стандарти 802.11r, 802.11v.

Складно обійтися без Mesh-систем в різнорівневих приміщеннях і великих офісах. Найпотужніші роутери створюють покриття до 200 м², якщо в приміщенні немає стін. Якщо площа більша або вам потрібно роздати Wi-Fi на кілька поверхів або кімнат, то навряд чи вийде обійтися без ретранслятора. Але навіть якщо один потужний роутер може забезпечити потрібне покриття, краще віддати перевагу кільком малопотужним точкам доступу. Розташовують їх на відстані мінімум 3 метра один від одного або через 2 цегляні/бетонні стіни.

Найкраще купувати Mesh систему комплектом, коли продається відразу кілька точок. Можна зібрати її самостійно, але при цьому потрібно враховувати сумісність і наявність потрібного ПЗ для керування та налаштування. В іншому випадку, навіть якщо зібрана безшовна система буде працювати, можливий згаданий ефект пляшкового горлечка.

Антени роутера

Антени збільшують дальність покриття бездротової мережі, не впливаючи на потужність самого сигналу. При цьому важливим є не кількість антен, а їх коефіцієнт посилення. Втім, він не може чітко позначити межі безпровідної мережі. Зате такої інформації буде достатньо для порівняння: ви будете розуміти, що маршрутизатор з посиленням 5 dBi «добиває» далі, ніж з 2,5 dBi. Більшість роутерів мають вбудовані внутрішні антени, хоча деякі моделі можуть мати зовнішні антени або можливість підключення зовнішніх антен. Кількість антен може впливати на якість покриття і міцність сигналу. Існує кілька типів антен, які використовуються у роутерах, таких як дипольні антени, направлені антени, секторні антени тощо. Кожен тип антени має свої особливості, які впливають на напрямок та охоплення сигналу.

Рисунок 3.5 – Wi-Fi роутер із зовнішніми антенами

Антени стоять на всіх роутерах і бувають внутрішніми і зовнішніми. Зовнішні в свою чергу бувають знімними/незнімними, регульованими/нерегульованими.

Вбудовані антени зазвичай всеспрямовані, тобто поширюють сигнал однаково на всі боки (рис. 3.5). Зовнішні антени є секторними, тобто випромінюють сигнал тільки в певному напрямку. Це знижує охоплювану площу, але підвищує дальність сигналу. Деякі роутери підтримують заміну зовнішніх антен на більш потужні.

Напряму кількість антен не впливає на пропускну здатність, але вони дозволяють використовувати технологію MU MIMO, яка робить роутер швидшим.

Для роботи роутера потрібен мінімум 1 порт для підключення інтернету. Сьогодні стандартом є WAN-порт для оптоволоконного кабелю. Також маршрутизатори оснащуються вихідними LAN-портами для оптоволокна. Вони потрібні, якщо ви збираєтеся до деяких пристроїв підвести інтернет через кабель, і в цьому випадку маршрутизатор виконує функцію комутатора.

При виборі потрібно звертати увагу не тільки на наявність таких роз'ємів, але також і на їх характеристики, адже і через кабель, і через бездротову мережу передача даних має обмеження. Оптимальний варіант – стандарт 10/100/1000BASE-T Ethernet, який забезпечує передачу даних 1 Гбіт/с. Якщо у порту LAN стандарт 10/100BASE-T Ethernet, то її верхній поріг – 100 Мбіт/с.

Практично всі сучасні моделі роутерів мають порт USB. Часто його не використовують, але іноді роз'єм корисний. Наприклад, в офісі через USB підключають принтер, і тоді роздрукувати документи зможе будь-який із комп'ютерів з доступом. Також через роз'єм USB підключають SSD, який виконує функцію зовнішнього сховища (рис. 3.6).

Рисунок 3.6 – SSD сховище для роутера

3.5 Організація радіус сервера

Функції сервера Radius

Серед його характеристик виділяється гнучкість і потужність, якими він володіє в процесі управління. Цей протокол дозволяє вам керувати всією мережею в будь-який час, від моменту початку сеансу до завершення процесу перегляду мережі. і Ви маєте можливість виставляти рахунок за використані мегабайти. Це дуже універсальна система і працює через порт UDP 1812, де багато маршрутизаторів можуть мати цю послугу, доступну для користувачів, вона також може використовуватися в серверах OLT або NAS і має багато можливостей для будь-якого користувача, який хоче її встановити. Механізм аутентифікації, що використовується для спільних ресурсів, дозволяє авторизувати користувачеві, щоб увійти до нього, але він повинен виконувати певні операції, такі як облік, аналіз управління та реєстрація статистики, які пізніше використовуються для стягнення плати або звітування про стан системи та використання.

Він застосовується в домашніх маршрутизаторах тих користувачів, які аутентифікують його для доступу в Інтернет.

3.6 Реалізація контролера радіоспотів на роутері рівня L2\L3 Mikrotik

MikroTik є популярним виробником мережевих пристроїв, включаючи роутери рівня L2/L3. Їх пристрої пропонують широкий спектр функцій і можливостей для управління і налаштування мережі. Основні характеристики роутерів MikroTik рівня L2/L3 включають (рис. 3.7).

Протоколи маршрутизації: MikroTik підтримує різні протоколи маршрутизації, такі як RIP (Routing Information Protocol), OSPF (Open Shortest Path First), BGP (Border Gateway Protocol) та інші. Це дозволяє створювати складні мережі і налаштовувати маршрутизацію між ними.

Рисунок 3.7 – комутатор рівня L2

VLAN (Virtual Local Area Network): Роутери MikroTik підтримують VLAN, що дозволяє створювати віртуальні локальні мережі для розділення трафіку і керування доступом.

Firewall (брандмауер): MikroTik має розширені можливості в області брандмауера, що дозволяє контролювати і фільтрувати трафік, налаштовувати правила безпеки і забезпечувати захист мережі.

VPN (Virtual Private Network): Роутери MikroTik можуть працювати як VPN-сервери або клієнти, дозволяючи забезпечити зашифроване з'єднання і безпеку при підключенні до віддалених мереж.

VPN-сервер - це сервер, який забезпечує можливість встановлення віртуальної приватної мережі (VPN) для з'єднання клієнтських пристроїв з інтернет-мережею. Він виконує роль посередника між клієнтами і мережею, забезпечуючи безпечний і зашифрований обмін даними. VPN-сервери здійснюють аутентифікацію користувачів, перевіряючи їхні облікові дані, такі як ім'я користувача і пароль. Після успішної аутентифікації VPN-сервер визначає права доступу користувача до ресурсів мережі. VPN-сервери забезпечують шифрування даних, що передаються між клієнтами і сервером, для забезпечення конфіденційності та захисту від несанкціонованого доступу. Зазвичай використовуються протоколи шифрування, такі як IPSec, SSL/TLS або OpenVPN. VPN-сервери створюють віртуальний тунель між клієнтами і сервером, який дозволяє передавати дані через незахищені мережі, такі як Інтернет, у безпечному зашифрованому вигляді. Це дозволяє користувачам отримувати доступ до ресурсів мережі з будь-якого місця і забезпечує їх безпеку. VPN-сервери можуть бути масштабовані, щоб обробляти велику кількість одночасних з'єднань від клієнтів. Це важливо для організацій, які потребують великої кількості з'єднань від своїх співробітників.

Quality of Service (QoS): MikroTik дозволяє налаштовувати QoS для пріоритезації трафіку і забезпечення вимог щодо якості обслуговування, що допомагає керувати пропускною здатністю мережі і забезпечити надійність послуг.

Комутатор L2 обробляє та реєструє MAC адреси кадрів, здійснює фізичну адресацію та управління потоком даних. Деякі додаткові функції: VLAN, QoS підтримуються лише на рівні, необхідному для передачі параметрів або участі у загальній схемі мережі. Наприклад, на комутаторі L2 можна прописати кілька VLAN, але не можна налаштувати повноцінну маршрутизацію між ними, для цього вже потрібний комутатор L3. Простіше кажучи, комутатор рівня L2 забезпечує деякі додаткові функції, але не керує ними в масштабі мережі.

На відміну від своїх простіших побратимів, комутатори L3 можуть брати на себе функції маршрутизаторів, у тому числі перевірку логічної адресації та вибір шляху (маршруту) доставки даних. Завдяки повсюдному впровадженню стека протоколів TCP/IP, комутатори рівня L3 (рис. 3.8) є важливою частиною мережі, оскільки можуть виконувати пересилання пакетів не тільки на основі аналізу MAC адрес, але й «піднімаючись на поверх вище», тобто на основі IP адрес та відповідних протоколів маршрутизації.

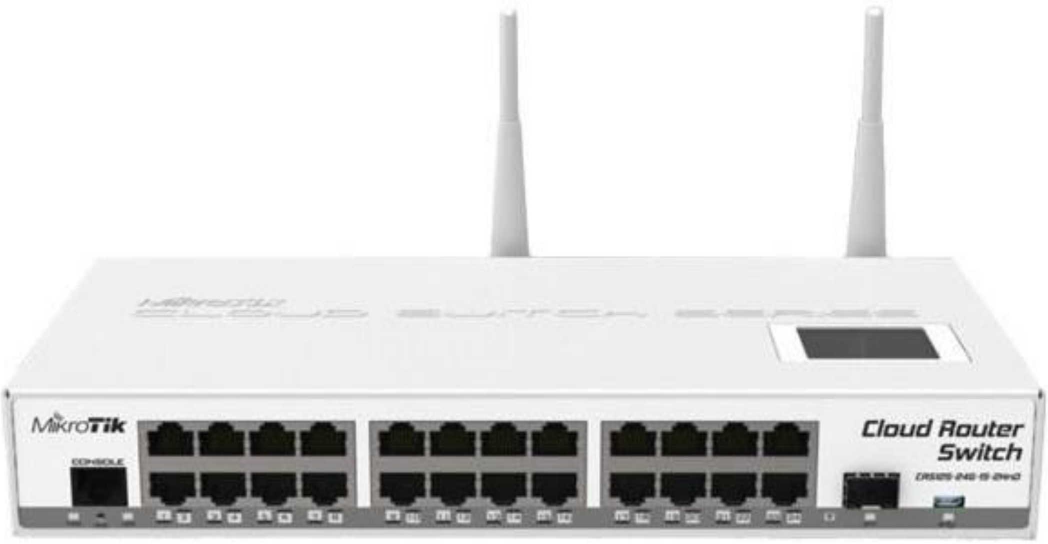


Рисунок 3.8 – комутатор рівня L3

Зрозуміло, нікому на думку не спаде будувати зовнішню розгалужену мережу з BGP маршрутизацією на базі комутаторів. Однак для внутрішньої маршрутизації у межах локальної мережі такий варіант цілком підходить. Мало того, це дозволяє заощаджувати придбання додаткових пристроїв (маршрутизаторів), використовувати універсальний підхід до організації мережі.

Через підтримку багатьох функцій комутатор рівня L3 мають складнішу внутрішню конфігурацію і, відповідно, коштують дорожче. Іноді користувач постає перед вибором: купити простіший і бюджетніший варіант з Layer 2 або дорожчий і «просунутий» Layer 3.

Комутатори, які служать для об'єднання інших комутаторів у єдину мережу, називають комутатори рівня агрегації (або комутатори рівня розподілу).

Якщо говорити про рівень ядра мережі, то для нього існують свої потужні комутатори, основне завдання яких максимально швидко передавати трафік. Функції управління у своїй досить часто делегується до рівня агрегації.

Чи є зв'язок між поняттями рівнів L2 та L3 з рівнем доступу та рівнем агрегації? Традиційно вважається, що для рівня доступу краще підходять комутатори L2 (насамперед через нижчу ціну, а для рівня агрегації краще вибирати L3 заради підвищеної функціональності.

Чим добрий такий підхід? Встановлювати більш функціональні та дорогі комутатори рівня L3 на рівні доступу може бути невиправданим кроком, якщо їх функції маршрутизації та контролю не будуть потрібні. А цих же функцій бракуватиме простішим комутаторам L2 лише на рівні агрегації (розподілу).

Якщо є сумніви який рівень комутатора вибрати: рівня 2 або рівня 3, в основу потрібно ставити питання, де його передбачається використовувати. Якщо є лише невелика мережа, що дозволяє всім працювати в єдиному широкомовному домені, можна зупинити свій вибір на одному або двох комутаторах L2.

Другий випадок, де комутатори другого рівня добре почуваються - рівень доступу, тобто там, де комп'ютери користувачів підключаються до локальної мережі.

Якщо потрібний комутатор для об'єднання (агрегування) кількох простих комутаторів доступу користувачів — для цієї ролі краще підходить комутатор рівня 3. Крім об'єднання в мережу, він може виконувати маршрутизацію між VLAN, керувати проходженням трафіку за допомогою ACL (Access Control List), забезпечувати заданий рівень ширини пропускання (QoS) тощо.

Ще одна область, де комутатори L3 часто бувають затребувані - якщо необхідно забезпечити підвищені вимоги до безпеки, наприклад, більш гнучке розмежування доступу. Деякі функції, доступні для цього рівня, наприклад, управління трафіком на рівні IP адрес, будуть нездійсненні стандартними засобами рівня L2.

3.7 Система моніторингу та аналізу

Система моніторингу та аналізу системи RADIUS (Remote Authentication Dial-In User Service) допомагає відстежувати та аналізувати активність, події та статистику, пов'язані з RADIUS-сервером. Така система може надати операторам мережі цінну інформацію про використання ресурсів, проблеми безпеки та продуктивність системи RADIUS. Систему моніторингу та аналізу (рис. 3.9) краще всього реалізувати на невеликому сервері або навіть ПК достатньої потужності з відповідним ПЗ.

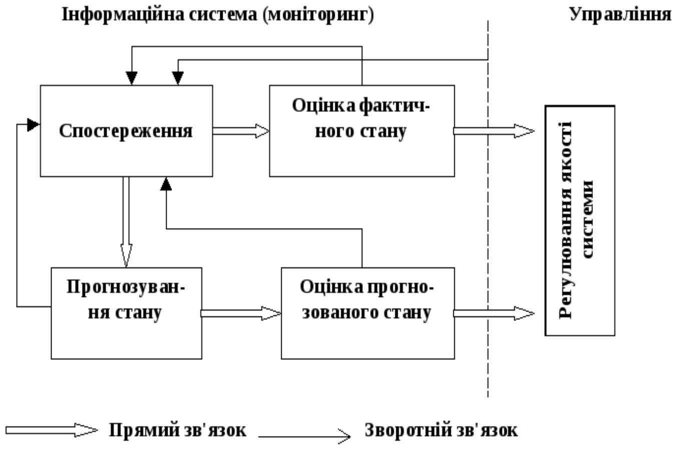


Рисунок 3.9 - Система моніторингу та аналізу системи RADIUS

На даний момент для організацій, що використовують мережу з комутацією пакетів, задається ряд вимог щодо забезпечення інформаційної безпеки як користувальницької, так і службової інформації. Однією з таких вимог є створення централізованого сервісу аутентифікації, авторизації та обліку подій при віддаленому доступі до вузла комутації МКП (мережа з комутацією пакетів). Цей сервіс розгортається з урахуванням сервера AAA (Authentication, Authorization, Accounting).

На базі апаратного забезпечення та програмного забезпечення ОС Windows 7 із встановленими програмними продуктами WMware Workstation і GNS3 було розгорнуто стенд емулюючий віддалений доступ на вузол комутації СКП, використовуючи групу серверів RADIUS (Remote Authentication Dial In User Service). Додавання сервера RADIUS з відкритим програмним кодом передбачається на базі ДОС (довірена операційна система) Astra Linux SE. Однак у ДОС Astra Linux SE не вбудований пакет установки FreeRadius, для реалізації стенду було висунуто ОС (операційна система) Debian і її основі було розгорнуто сервер RADIUS. Для емуляції LAN-мережі використали образ маршрутизатора Cisco c7200.

Емуляція відключення функціонування основного RADIUS-сервера.

Після відключення основного сервера-RADIUS Debianl0.64-bit-l спроби віддаленого входу на один з мережевих пристроїв призвели до того, що маршрутизатор спочатку посилав пакети RADIUS на основний сервер і після кількох спроб і неотримання відповіді від основного сервера RADIUS, пристрій починає відправляти RADIUS -пакети на другорядний сервер.

Альтернативна конфігурація передбачає, що вхід на мережевий пристрій під обліковим записом, що зберігається на мережному пристрої, буде неможливий, якщо основний та резервний RADIUS-сервер будуть функціонувати. Тим самим унеможливлюється порушника безпосередньо взаємодіяти з мережевим пристроєм, а самі RADIUS-сервери передбачається оснастити сервісами безпеки для виявлення підозрілих запитів та мережевих атак.

3.8 Основні поняття AAA

Аутентифікація (authentication) – визначення особистості того, хто намагається поринути у приміщення. У нашому прикладі це може бути сканування відбитка пальця, адже у кожної людини він є унікальним і може бути гарантом підтвердження особистості. У мережному світі стандартна автентифікація полягає у використанні логіну та паролю, які згенеровані для кожного користувача і дозволяють йому підтвердити свою особистість.

Авторизація (authorization) – наступний крок після успішної автентифікації. Полягає у перевірці прав доступу до приміщення тієї людини, яка пройшла автентифікацію. Можливо, людина має право проникнути в перше приміщення, але заборонено проходження далі. На мережних пристроях права доступу найчастіше визначають перелік команд, які може виконати користувач, який пройшов аутентифікацію. Наприклад, мережному інженеру з 1-м рівнем доступу дозволено лише перегляд конфігурації пристрою за допомогою команди show, а інженеру з 2-м рівнем доступне внесення змін. На AAA-серверах операторів зв'язку (рис. 3.10) право доступу може визначати належність абонента до будь-якого тарифного плану.

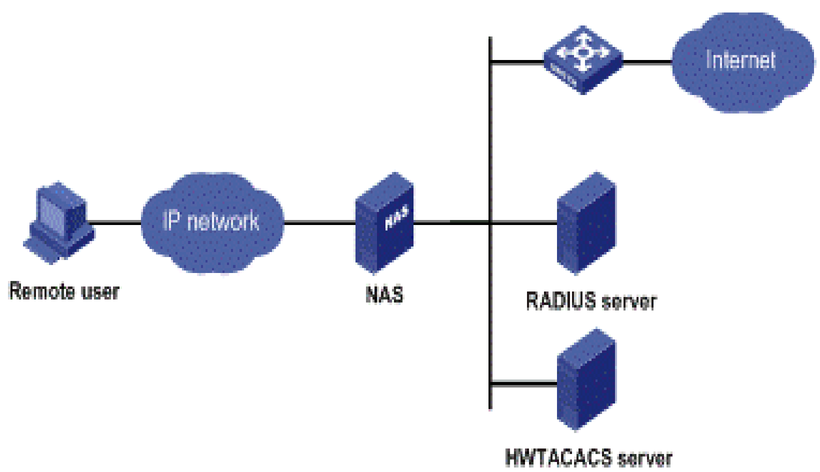


Рисунок 3.10 – AAA-server

Облік (accounting) – паралельний з автентифікацією та авторизацією етап, який записує в журнал успіх чи невдачу даних процесів, зміг людина проникнути в приміщення чи ні, чи отримав користувач доступ до мережного пристрою і, якщо так, то які дії на ньому робив. Цей процес важливий з точки зору безпеки та контролю доступу, оскільки дозволяє визначати потенційні загрози та шукати «дірки» в системі.

Протокол RADIUS є стандартом IETF для AAA. Використовується з початку 1990-х років і спочатку застосовувався для модемних комутованих з'єднань. Спочатку використовувався для розширення Layer 2 протоколу точка-точка (PPP) між кінцевим користувачем та сервером доступу до мережі (NAS), передаючи трафік автентифікації з NAS на сервер AAA. Відомості від автентифікації та авторизації доставляють одним типом пакетів, а облік обробляється окремим процесом. RADIUS має широке поширення та підтримується більшістю виробників пристроїв та розробників програмних продуктів.

Сучасна реалізація RADIUS використовує порти 1812 (аутентифікація) та 1813 (облік) протоколу UDP (також можливе використання портів 1645 та 1646). UDP має високу швидкість, але має ряд недоліків, які необхідно враховувати при його застосуванні. Коли розробляли RADIUS, питання безпеки не були настільки актуальними, як зараз, тому він підтримує досить малу кількість типів аутентифікації (Clear text і CHAP), шифрує лише поле з паролем і загалом має середній рівень безпеки. UDP (User Datagram Protocol) - це протокол на транспортному рівні в моделі OSI (Open Systems Interconnection). Він забезпечує ненадійну доставку даних між додатками в мережі. UDP використовується для передачі даних без необхідності встановлення надійного з'єднання. UDP не гарантує надійну доставку даних. Це означає, що він не здійснює перевірку доставки, повторну передачу пакетів чи контроль за порядком приймання даних. Якщо пакети втрачаються або приходять у неправильному порядку, відповідальність за обробку цього лежить на додатку, що працює з UDP. UDP є простим протоколом, що призводить до меншої накладної на зв'язок порівняно з протоколами, такими як TCP (Transmission Control Protocol). Відсутність механізмів, які забезпечують надійність, дозволяє UDP передавати дані швидше. Заголовок UDP містить мінімальну кількість інформації, необхідної для передачі даних. Це дозволяє скоротити розмір пакетів та зменшити накладні витрати мережевих ресурсів. UDP не встановлює з'єднання між відправником та отримувачем перед передачею даних. Це означає, що пакети можуть бути надіслані на будь-яку IP-адресу і порт без попереднього обміну сигналами для встановлення з'єднання.

3.9Висновки

Проведено апаратну реалізацію системи управління. Розглянуто основні характеристики, виявлено базові потреби для організації радіус сервера. Розроблено систему моніторингу та аналізу. Підключено і налаштовано сервер RADIUS, виявлено характеристики якими він володіє. Перевірені популярні виробники мережевих пристроїв та їх надійність і недоліки.

ВИСНОВКИ

Сучасний світ дав зрозуміти для нас, що розповсюдження бездротових мереж є необхідним. Це і призвело до розробки бездротових технологій і їх подальшого вдосконалення. Одна із таких систем RADIUS (Remote Authentication Dial-In User Service). Система забезпечила автентифікацію, авторизацію, облік користувачів щодо доступу до Wi-Fi мережі. Ми розібрали як працює точка доступу Wi-Fi, яка використовує безпечну систему управління RADIUS. Ми дізнались як система спрощує управління точками доступу Wi-Fi шляхом автоматизації, яке до цього адміністратор виконував вручну. Використовуючи систему управління RADIUS, система може гарантувати надання доступу лише для авторизованих користувачів. Система RADIUS масштабується, її використовують як поодинокі унікальні користувачі, так і школи, університети та корпоративні середовища.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Подчашинський Ю.О. Проектування комп’ютеризованих систем управління технологічними процесами : навч. посібник. – Житомир : ЖДТУ, 2018. – 200 с.

2. Матвієнко М.П. Комп'ютерна схемотехніка: навчальний посібник. Київ: ТОВ "Центр навчальної літератури", 2019. 165 с.

3. Як налаштувати бездротову мережу WPA2-Enterprise за допомогою RADIUS Server на Synology Router?[Електронний ресурс]. http://fnb.ua/index.php?newsid=59 (дата звернення 01.06.2023).

4. Красніков А.С. «Побудова захищеної Wi-Fi мережі з застосуванням Radius сервера» навч. Посібник. – Суми: СумДУ, 2019. – 180 с.

5. Вишня В. Б. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. навч. Посібник . Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

6. Коваль Ю. В. інформаційні мережі Навчальний посібник – Київський Національний Університет імені Тараса Шевченка. Київ, 2021. – 84 с.

7. Сасюк В. О. Безпровідна комп'ютерна мережа на основі стандарту 802.11ac. Тернопільський національний економічний університет. 2018.-105 с.

8. Третяк М.І. «Розробка програмного забезпечення для централізованого збору оповіщень з використанням хмарних технологій». Вінницький національний технічний університет. Вінниця 2022. - 185 с.

9. Зацерковний В.І. Обчислювальна техніка: історія розвитку від найпростіших пристроїв для лічби до електромеханічних комп’ютерів: монографія. Ніжин: Аспект-Поліграф, 2012. 416 с.

10. Бєліков Д.О. Кафедра інформаційних систем та технологій. Національний технічний університет «Дніпровська політехніка». Дніпро 2020. - 77 с.

11. Боярська К.М. ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ“ Тенденції розвитку засобів захисту інформації бездротових комунікаційних систем” Київ – 2021. – 85 с.

12. Юглічек О.В. Засоби захисту комп'ютерної мережі з використанням обладнання Cisco/ Computer network security tools based on Cisco mains Тернопільський національний економічний університет. Тернопіль – 2018 225 с.

13. Василенко М. Ю. «Графічний інтерфейс інтелектуальної системи керування трансляцією мережевих адрес на основі протоколу NAT» Сумський Державний Університет Суми 2020. - 135 с.

14. Christian Jacquenet, Gilles Bourdon, Mohamed Boucadair Control and Provisioning of Wireless Access Points (CAPWAP) 2021.

15. AAA (Authentication, Authorization, Accounting) – Cisco URL: https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html (Дата зверенння: 16.05.20203)

16. AAA (Authentication, Authorization, Accounting) – TechTarget URL: https://searchnetworking.techtarget.com/definition/AAA (Дата звернення: 16.05.2023)

17. Understanding AAA (Authentication, Authorization, and Accounting) - Palo Alto Networks URL: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/understanding-aaa-authentication-authorization-and-accounting.html (Дата звернення 17.05.2023)

18. AAA Services - Juniper Networks URL: https://www.juniper.net/documentation/en_US/junos/topics/concept/security-aaa-services-overview.html (Дата звернення 17.05.2023)

19. Introduction to AAA (Authentication, Authorization, and Accounting) – FortinetURL: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/589154/authentication-authorization-and-accounting (Дата звернення 17.05.2023)

20. Довбиш А.С. «Побудова захищеної Wi-Fi мережі з застосуванням Radius сервера» СУМИ 2020. - 205 с.

21. Божко В. В. РОЗРОБКА ЗАСТОСУВАННЯ ДЛЯ ПРОЕКТУВАННЯ, ВІДОБРАЖЕННЯ ТА АНАЛІЗУ ER-МОДЕЛЕЙ. НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ» Київ 2020. – 135 с.

22. Палажченко Є. В. «Інформаційна система моніторингу показників стану повітря в приміщенні» СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ Суми-2020 – 165 с.

23. Авраменко В.С. «проектування інформаційних систем» ЧЕРКАСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ БОГДАНА ХМЕЛЬНИЦЬКОГО Черкаси 2019 – 205 с.

24. Сердюк О. О. «Цифрові системи керування й обробки інформації» Донбаська державна машинобудівна академія Кафедра автоматизації виробничих процесів. Краматорськ 2018. – 155 с.

25. Волощук В. А. «Проєктування інформаційних систем» «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО» Київ 2022. – 55 с.

26. TP-Link URL: https://www.tp-link.com/us/home-networking/wifi-router/ (Дата звернення 21.05.2023)

27. NETGEAR URL: https://www.netgear.com/home/products/networking/wifi-routers/ (Дата звернення 21.05.2023)

28. ASUS URL: https://www.asus.com/Networking-IoT-Servers/WiFi-Routers-Products/ (Дата звернення 21.05.2023)

29. Linksys URL: https://www.linksys.com/us/wireless-routers/ (Дата звернення 22.05.2023)

30. D-Link URL: https://www.dlink.com/en/products/routers (Дата звернення 22.05.2023)

31. What is a Mesh Wi-Fi System? – PCMag URL: https://www.pcmag.com/picks/the-best-wi-fi-mesh-network-systems (Дата звернення 22.05.2023)

32. How Does Mesh Wi-Fi Work? – Lifewire URL: https://www.lifewire.com/what-is-mesh-wifi-4683897 (Дата звернення 22.05.2023)

33. Mesh Networking Explained – NETGEAR URL: https://www.netgear.com/home/discover/wifi/mesh-wifi/ (Дата звернення 22.05.2023)

34. What Is a Mesh Network and How Does It Work? – Linksys URL: https://www.linksys.com/us/r/resource-center/what-is-a-mesh-network/ (Дата звернення 22.05.2023)

35. The Benefits of a Mesh Wi-Fi Network – Lifewire URL: https://www.lifewire.com/mesh-wifi-network-benefits-4776360 (Дата звернення 22.05.2023)

36. Cisco Wireless LAN Controller Configuration Guide URL: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810.html (Дата звернення 26.05.2023)

37. ArubaOS User Guide - Configuring the Controller URL: https://www.arubanetworks.com/techdocs/ArubaOS_63_Web_Help/Content/ArubaFrameStyles/Command_Lists/Configuring_the_Controller.htm (Дата звернення 26.05.2023)

38. ExtremeWireless WiNG 7.x Configuration Guide URL: https://www.extremenetworks.com/resources/extremewireless-wing-7-x-configuration-guide/ (Дата звернення 29.05.2023)

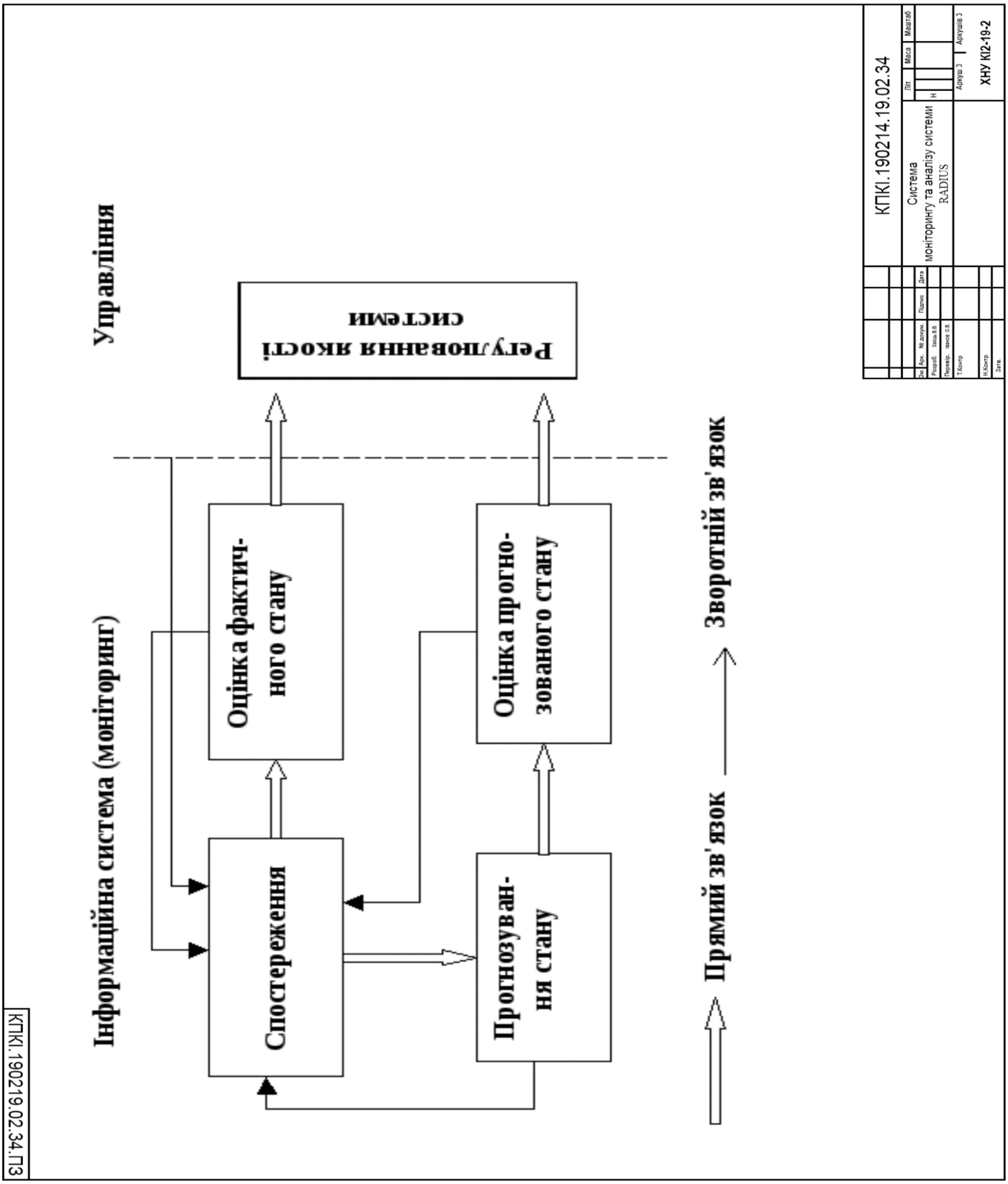
39. Configuring the Ruckus Wireless ZoneDirector URL: https://docs.commscope.com/bundle/zoneflex-t300e-zonecontroller-product-reference-guide/page/GUID-63314A29-816A-4B2A-A20B-A3F2499C08D0.html (Дата звернення 29.05.2023)

40. Aerohive HiveManager NG Configuration Guide URL: https://www.extremenetworks.com/resources/aerohive-hivemanager-ng-configuration-guide/ (Дата звернення 29.05.2023)

Додаток А

(обов’язковий)

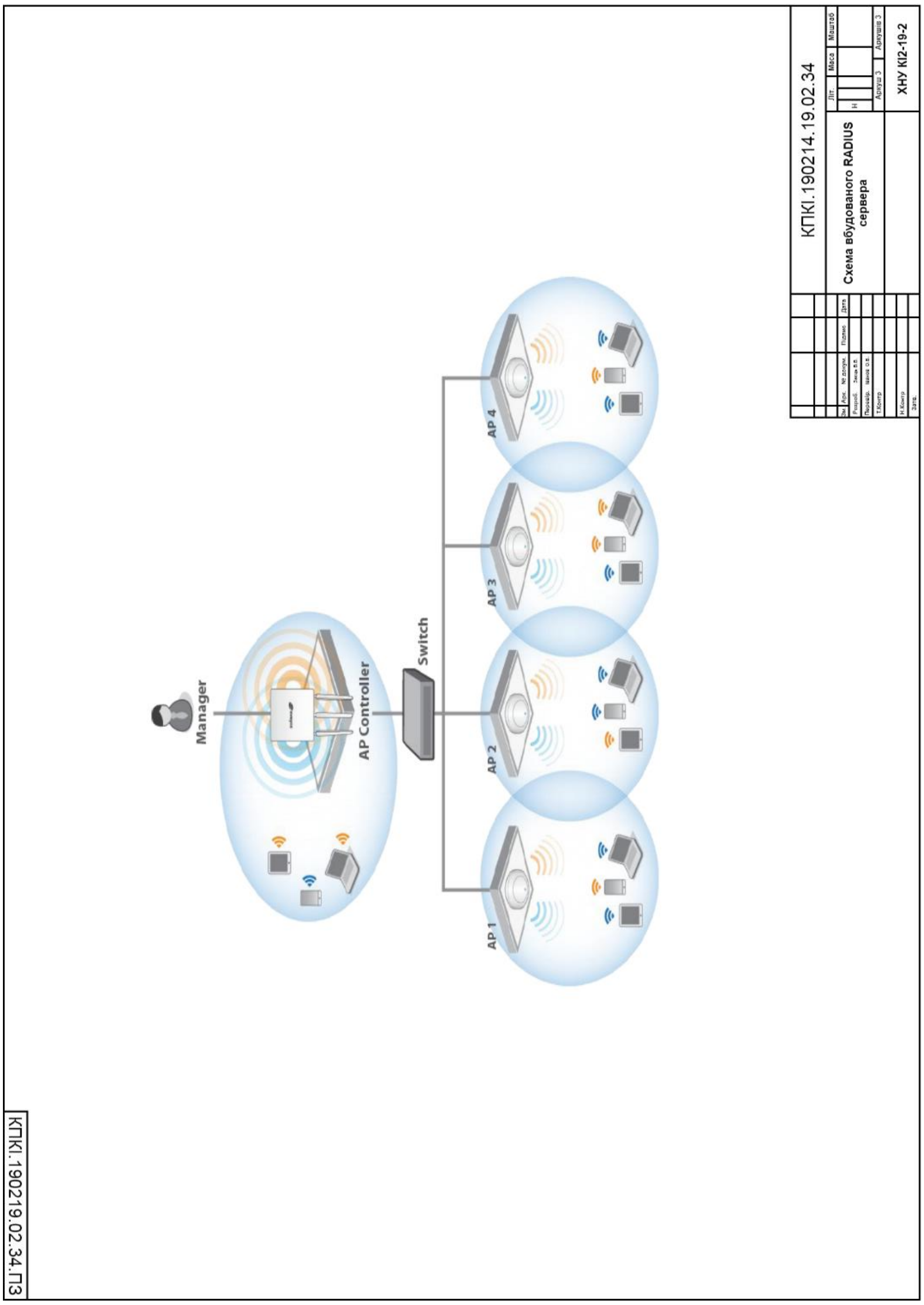
Копія креслення «Система моніторингу та аналізу системи RADIUS»



Додаток Б

(обов’язковий)

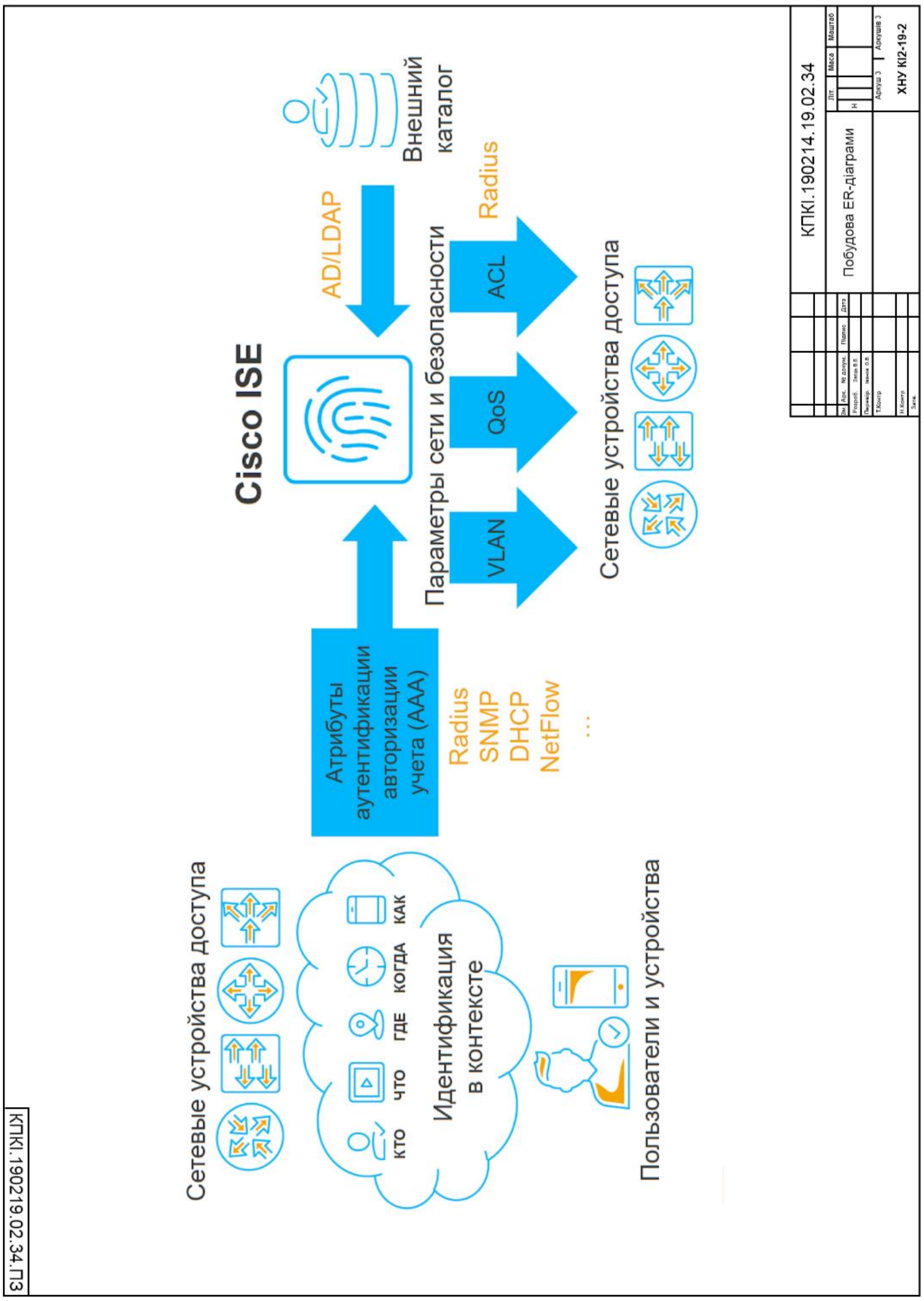
Копія креслення « Система вбудованого RADIUS сервера»



Додаток В

(обов’язковий)

Копія креслення «Побудова ER-діаграми»



UNICHECK

User name:
Кафедра КІ

Check date:
09.06.2023 11:00:49 EEST

Report date:
09.06.2023 11:11:59 EEST

Check ID:
1015522962

Check type:
Doc vs Internet + Library

User ID:
100005591

File name: **Заєць_Система управління Wi-Fi радіоспотами з використанням системи RADIUS**

Page count: **71** Word count: **11548** Character count: **92053** File size: **2.89 MB** File ID: **1015177175**

29.2% Matches

Highest match: **11%** with Internet source (**https://www.itbox.ua/ua/blog/Yak-vibrati-router-dlya-domu-kvartiri-ofisu**)

2.59% Quotes

0% Exclusions

No exclusions

Modifind

Text modifications detected. Find more details in the online report.

Replaced characters 2

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 7.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 10%**

	Документ		Сумарний збіг по Базі Даних	
ID: 115332 Назва: БКР Мультикомп'ютерна система згідно топології «потовщене дерево» Додано в БД: 2023-06-08 Автора: Б. Р. Трет'яков Керівники: К. М. Березька Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	86783	704	9801 (11%)	83 (12%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Заєць Віталій Вікторович

Тема: Система управління Wi-Fi радіоспотами з використанням системи RADIUS

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень ___3____ Кількість сторінок записки ___61___

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є проектування та моделювання системи управління Wi-Fi радіоспотами з використанням системи RADIUS.

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: В першому розділі кваліфікаційної роботи проведено дослідження предметної області (проаналізовано аспекти та особливості системи управління) та виконано постановку задачі дослідження. В другому розділі кваліфікаційної роботи проведено проєктування системи управління з використанням системи RADIUS а саме: виконано опис системи RADIUS; розроблено структурну схему мережі; визначено необхідне апаратне та програмне забезпечення: В третьому розділі кваліфікаційної роботи проведено моделювання системи управління Wi-Fi радіоспотами з використанням системи RADIUS, а саме: реалізовано апаратну модель RADIUS сервера. Розроблено проміжне програмне забезпечення.

4. Позитивні сторони роботи: висока практична цінність роботи.

5. Негативні сторони роботи: недостатня увага опису проміжного програмного забезпечення.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на належному науково-технічному рівні.

8. Інші зауваження: ______

9. Оцінка дипломної роботи:

Розглянувши позитивні та негативні сторони представленої дипломної роботи вважаю, що робота заслуговує оцінки «добре» 3,75(С)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) ______

Кльоз Юрій Павлович, завідувач кафедри кібербезпеки, к.т.н, доцент

______(підпис)

"23" 06 2023 р.

Завідувачу кафедри КІС
д-р.техн.наук, проф. Говорущенко Т. О.

Зайця Віталія Вікторовича
ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи КІ2-19-2

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

22 квітня 2023 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ
КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система управління Wi-Fi радіоспотами з використанням системи RADIUS

Автор: Заєць Віталій Вікторович

Спеціальність: 123 – Компютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Іванов Олексій Валентинович, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-30 джерелами на один фрагмент речення;

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ідентичності/схожості, складає 29.2% і адресується до 453 першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи	____________	О. В. Іванов
Гарант ОП	____________	С. М. Лисенко
Завідувач кафедри КІІС	____________	Т. О. Говорущенко