ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Впровадження хмарної архітектури Cisco в безпроводові комп'ютерні мережі»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерна інженерія
освітньо-професійної програми Комп'ютерна інженерія

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Дмитро МАЙСТРЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Виконав: здобувач вищої освіти
групи КІД-42
Дмитро МАЙСТРЕНКО

Керівник: Юлія БОРОВА

Рецензент: _____

Київ – 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут інформаційних технологій

Кафедра Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 Комп'ютерна інженерія

Освітньо-професійна програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувачка кафедрою КІ
_____ Наталія ЛАЩЕВСЬКА
« » _____ 2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Майстренку Дмитру Васильовичу

1. Тема кваліфікаційної роботи: «Впровадження хмарної архітектури Cisco в безпроводові комп'ютерні мережі»,
керівник кваліфікаційної роботи Юлія БОРОВА, асистент,
затверджені наказом Державного університету інформаційно-комунікаційних технологій від 27.02.2024 р. №36.

2. Строк подання кваліфікаційної роботи 10.05.2024 р.

3. Вихідні дані до кваліфікаційної роботи:
   1. Архітектура Cisco Meraki.
   2. Хмарний сервіс Cisco Meraki Cloud Manager.
   3. Обладання Cisco Meraki.
   4. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
   1. Складові елементи та переваги архітектури Cisco Meraki;
   2. Розгортання архітектури Cisco Meraki;
   3. Робота з хмарним сервісом управління Cisco Meraki Cloud Manager.

5. Перелік ілюстративного матеріалу: презентація.

6. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Підбір науково-технічної літератури	08.03.24	
2.	Складові елементи та переваги архітектури Cisco Meraki	22.03.24	
3.	Розгортання архітектури Cisco Meraki	05.04.24	
4.	Робота з хмарним сервісом управління Cisco Meraki Cloud Manager	19.04.24	
5.	Висновки, вступ, реферат	03.05.24	
6.	Розробка презентації	10.05.24	

Здобувач вищої освіти Дмитро МАЙСТРЕНКО

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи Юлія БОРОВА

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти Майстренка Дмитра Васильовича

на тему: «Впровадження хмарної архітектури Cisco в безпроводові комп'ютерні мережі»

Актуальність:

Архітектура Cisco Meraki надає готовий набір інструментів і рішень для більшості ситуацій. Відмінною особливістю даної архітектури є інтеграція точок доступу з хмарним середовищем Cisco Meraki Cloud Manager, що робить управління мережею простим з любої точки світу. А дослідження в цьому напрямку проведені в бакалаврській роботі, є актуальними.

Позитивні сторони:

Робота викладена науковою мовою, логічно й послідовно відбиває мету та поставлені в роботі завдання. Пояснювальна записка відповідає стандартам до її оформлення.

Проведені дослідження свідчать про високий науково-технічний рівень використання інформаційних технологій в даній роботі.

Недоліки:

1. В роботі завищений рівень опису процесу моніторингу та аналітики комп'ютерної мережі.
2. В роботі не описана архітектурна інтеграція Cisco Meraki з хмарою.

Висновок: кваліфікаційна робота заслуговує оцінку «відмінно», а здобувач Майстренко Дмитро Васильович заслуговує присвоєння кваліфікації: «бакалавр з комп'ютерної інженерії».

Рецензент: _____

(науковий ступінь, вчене звання) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут інформаційних технологій

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Майстренко Д.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)

за спеціальністю 123 Комп'ютерна інженерія
освітньо-професійної програми Комп'ютерна інженерія

на тему: Впровадження хмарної архітектури Cisco в безпроводові комп'ютерні мережі

Кваліфікаційна робота і рецензія додаються.

Директор ННІІТ _____ Андрій БОНДАРЧУК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Майстренко Дмитро Васильович показав гарну теоретичну та інженерну підготовку, уміння володіти технологіями нового покоління, вміло працювати з комп'ютерними програмно-апаратними засобами, довідковою і науково-технічною літературою. Працюючи над завданнями, які доручались керівником, проявив ініціативність, сумлінність та хист до інженерної роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу Майстренка Дмитра Васильовича на оцінку «відмінно» та присвоїти йому кваліфікацію «бакалавр з комп'ютерної інженерії».

Керівник кваліфікаційної роботи _____ Юлія БОРОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

" " _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Майстренко Д.В.
(прізвище та ініціали)

допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувачка кафедрою
Комп'ютерної інженерії _____ Наталія ЛАЩЕВСЬКА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

" " _____ 2024 року

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 57 стор., 38 рис., 17 дж.

Мета роботи - дослідження архітектури Cisco Meraki та робота з її складовими елементами.

Об'єкт дослідження - процес взаємодії складових елементів архітектури Cisco Meraki.

Предмет дослідження - архітектура Cisco Meraki.

Короткий зміст роботи: В бакалаврській роботі проаналізовано пристрої Cisco Meraki, як основний принцип побудови локальної мережі, для організації ефективного функціонування та спрощеного адміністрування мережі.

Практична частина роботи полягає у налаштуванні програмного забезпечення точок доступу Cisco Meraki та дослідженні хмарного сервісу управління Cisco Meraki Cloud Manager.

Зроблено висновок, що дана архітектура є гарним вибором в розширенні або побудові комп'ютерної мережі в цілому. Досліджено та запропоновано до реалізації архітектуру Cisco Meraki, як лінійку провідних рішень на ринку для організації безпечних і високонавантажених Wi-Fi-мереж. Визначено, що побудовані за допомогою Cisco Meraki безпроводові мережі прості в розгортці, легкі в управлінні, надійні, піддаються масштабуванню і працюють безвідмовно.

КЛЮЧОВІ СЛОВА: CISCO MERAKI, АРХІТЕКТУРА, ТОЧКИ ДОСТУПУ, НАЛАШТУВАННЯ, АПАРАТНЕ ЗАБЕСПЕЧЕННЯ, CISCO MERAKI CLOUD MANAGER, АНАЛІТИКА.

ЗМІСТ

ВСТУП

Сьогодні інформація відіграє важливу роль у житті та бузнесу, диктуючи умови роботи і розвитку. Людина є частиною глобального інформаційного середовища на підсвідомому рівні, оскільки на своєму життєвому шляху постійно стикається з різноманітними джерелами інформації. Водночас, в умовах розвитку інформаційних технологій процеси пошуку та обробки інформації прискорюються, що полегшує отримання будь-якого джерела інформації [1, 2].

Загалом процес становлення інформаційного суспільства в Україні та світі поступово розгортається. Водночас економічними передумовами цього процесу є техніко-технологічні засоби виробництва, пошуку та поширення інформації шляхом формування та застосування інформаційно-комунікаційних технологій.

Все більше і більше місць комп’ютеризують цей аспект. Глобальний нетворкінг стає одним із обов’язкових факторів у бізнесі та громадських місцях. Сьогодні є багато технологічно просунутих користувачів, які знають про можливості сучасних технологій. Такі користувачі хочуть мобільності, свободи вибору комунікаційних пристроїв, надійного доступу до мереж передачі даних у будь-який час і в будь-якому місці, що забезпечує широку смугу пропускання та високий рівень якості обслуговування. Будь-якому користувачеві важливий тільки його термінал з пакетом додатків і можливістю виходу в Інтернет або ресурси компанії. Взагалі, самим користувачам абсолютно байдуже, як побудована мережева інфраструктура. Це завдання IT-служб підприємства або операторів зв'язку. Для вирішення проблеми високоякісних і недорогих безпроводових компонентів мережі передачі даних доступу та забезпечення мобільності технологія WiFi наразі є найкращою. По-перше, це пов'язано з широкою доступністю і дешевизною клієнтських пристроїв, а також умовно вільними частотами 2,4 ГГц і 5 ГГц. Не менш важливо, що інфраструктурне обладнання досягло високого рівня, залишаючись відносно дешевим [3].

Cisco є світовим лідером у сфері інформаційних технологій, який допомагає підприємствам скористатися можливостями майбутнього та власним прикладом

доводить, що, поєднуючи непов’язане, можна досягти вражаючих результатів. Хмарні пристрої Meraki забезпечують централізовану видимість і контроль проводових і безпроводових пристроїв Meraki без витрат і складності безпроводових контролерів або дублюючих систем керування. Хмарне управління інтегрується з повним спектром продуктів Meraki, щоб забезпечити універсальне, інтуїтивно зрозуміле, централізоване та масштабоване керування мережами будь-якого розміру та функцій.

Вивчення методів побудови комп’ютерних мереж на основі рішень Cisco Meraki визначає актуальність бакалаврської роботи.

Мета роботи. Дослідження архітектури Cisco Meraki та робота з її складовими елементами.

Об’єктом дослідження є процес взаємодії складових елементів архітектури Cisco Meraki.

Предметом дослідження є архітектура Cisco Meraki.

1 СКЛАДОВІ ЕЛЕМЕНТИ ТА ПЕРЕВАГИ АРХІТЕКТУРИ CISCO MERAKI

1.1 Основні особливості архітектури Cisco Meraki

Cisco Meraki представляє собою комплексне рішення для керування мережею, яке включає безпроводові точки доступу, комутатори, маршрутизатори безпеки (звані також забезпеченням безпеки мережі), камери спостереження та інші технології. Основною особливістю архітектури Meraki є її цілковито управління через хмару (cloud-managed), що дозволяє адміністраторам мережі керувати всією своєю інфраструктурою з одного централізованого веб-інтерфейсу.

Архітектура Cisco Meraki надає готовий набір інструментів і рішень для більшості ситуацій прямо з коробки. Це означає, що купуючи цей товар, вам не потрібно робити інші покупки та нести додаткові витрати. Розгортання мережі дуже просте. Придбане обладнання доставлено та встановлено на об’єкті [3] (рис. 1.1).

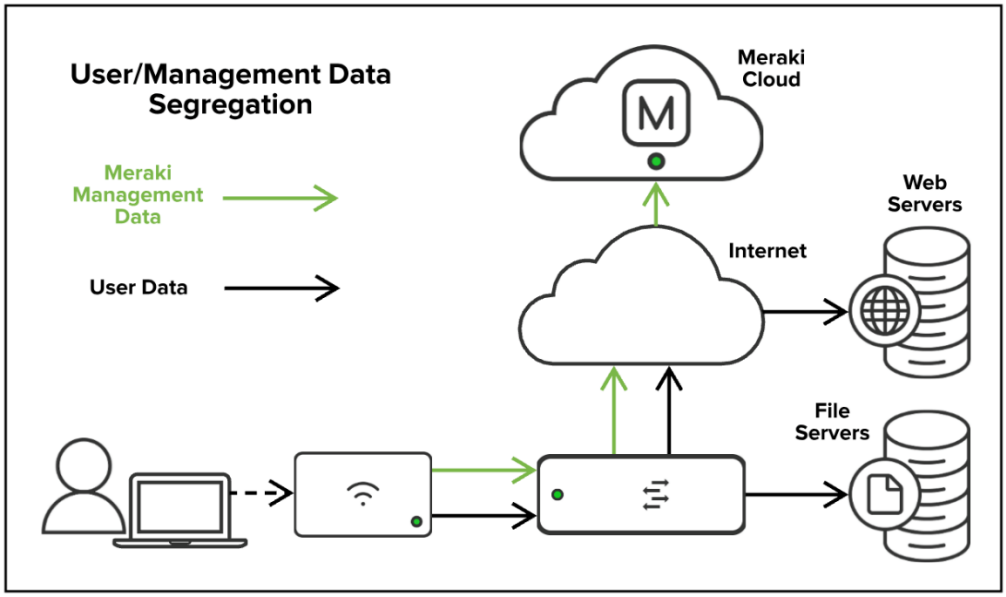


Рисунок 1.1 - Архітектура Cisco Meraki

Архітектура Meraki забезпечує багатофункціональне, універсальне

керування мережею без необхідності встановлення на місці контрольного обладнання та контролерів Wi-Fi.

Хмарне рішення Cisco Meraki — це централізована служба керування, яка дозволяє користувачам керувати всіма своїми мережевими пристроями Meraki за допомогою єдиної, простої та безпечної платформи.

Користувачі мають можливість встановлювати, керувати та настроювати своє обладнання Meraki за допомогою веб-інтерфейсу інформаційної панелі Meraki або API. Коли вони вносять зміни до налаштувань, запит на оновлення конфігурації відправляється до хмарної служби Meraki, яка потім розповсюджує ці зміни на відповідне обладнання.

Хмарна архітектура Cisco Meraki є основою рішення для керування Meraki. Ця «хмара» являє собою набір високонадійних багатокористувацьких серверів, стратегічно розподілених по всьому світу в центрах обробки даних Meraki. Сервери в цих центрах обробки даних є потужними хостинговими комп’ютерами, які складаються з багатьох окремих облікових записів користувачів. Вони називаються мультитенантними серверами, тому що облікові записи спільно використовують (рівні) обчислювальні ресурси на своєму хості (сервері). Однак, незважаючи на те, що ці облікові записи мають спільні ресурси, Meraki гарантує безпеку інформації клієнтів, обмежуючи доступ до організації на основі автентифікації облікового запису, а також хешуючи інформацію автентифікації, таку як паролі користувачів або ключі API.

Центри обробки даних. Дані керування клієнтами тиражуються в незалежних центрах обробки даних одного регіону в режимі реального часу. Ті самі дані також копіюються в автоматичних нічних архівних резервних копіях, які розміщуються сторонніми хмарними службами зберігання в регіоні. Хмара Meraki не зберігає дані користувачів клієнтів (рис. 1.2).

Центри обробки даних (ЦОД) — це спеціалізовані об'єкти, призначені для розміщення комп'ютерних систем та пов'язаного з ними компоненту, включаючи засоби зберігання даних та телекомунікаційне обладнання. ЦОД надають високий рівень безпеки, надійності доступу до даних і послуг, а також забезпечують

необхідне електроживлення, охолодження та підтримку зв'язку.

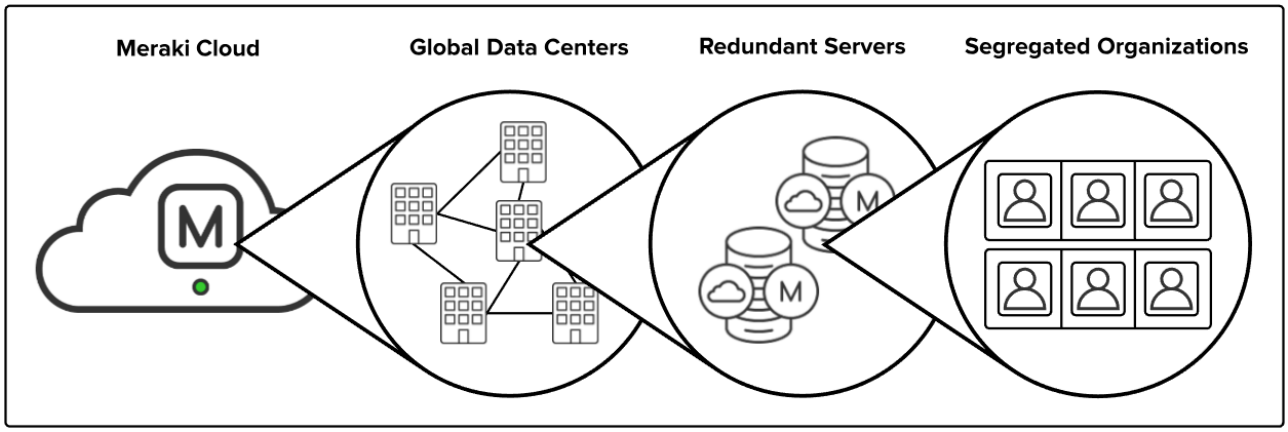


Рисунок 1.2 – Регіональний розподіл центрів обробки даних

Усі служби Meraki (інформаційна панель і API) також реплікуються в кількох незалежних центрах обробки даних, тому вони можуть швидко перемикатися після відмови в разі катастрофічного збою центру обробки даних.

Центри обробки даних Meraki розташовані по всьому світу, що забезпечує високу доступність локальних даних для суверенітету даних у чутливих країнах і регіонах, а також високошвидкісні з’єднання для забезпечення надійного хмарного керування зв’язком. Ці центри обробки даних мають такі сертифікати, як PCI, SAS70 Type II/SSAE, PCI та ISO27001 [4].

Кожен регіон (Північна та Південна Америка, Європа, Азія, Китай, Канада) має принаймні географічно відповідну пару (для відновлення після відмови) центрів обробки даних, де буде розташований основний сервер Meraki будь-якої кінцевої точки. У таблиці нижче вказано, які центри обробки даних охоплюють кожну область інформаційної панелі.

Під час створення облікового запису клієнти можуть вибрати, у якому регіоні розміщуватимуться їхні дані. Для клієнтів із глобально розосередженими мережами слід створити окремі організації для кожного регіону зберігання даних (Північна та Південна Америка, Європа, Азія, Китай і Канада). Регіон хостингу для кожного облікового запису можна знайти внизу сторінок інформаційної панелі Meraki, коли користувач увійшов.

Рисунок 1.3 – Розташування центрів обробки даних

Центр зберігання даних. Центри обробки даних Meraki містять активні дані конфігурації пристрою Meraki та історичні дані про використання мережі. Ці центри обробки даних містять кілька обчислювальних серверів, на яких зберігаються дані керування клієнтами. Ці центри обробки даних не зберігають дані користувачів клієнтів.

Meraki Device-to-Cloud Communications. Meraki застосовує механізм віддаленого виклику процедур (RPC), керований подіями, для зв'язку пристроїв Meraki з інформаційною панеллю та для обміну даними з серверами Meraki (див. рис. 1.4). Апаратні засоби Meraki функціонують як сервер/приймач, оскільки хмара Meraki ініціює виклики до цих пристроїв для збору даних та реалізації конфігурацій. Оскільки хмарна інфраструктура є ініціатором, конфігурації можна налаштовувати у хмарі навіть до того, як пристрої з'являться в мережі або будуть фізично встановлені.

У разі втрати підключення до хмари (що найчастіше спричинено локальним провайдером Інтернету або збоєм підключення), апаратний пристрій Meraki продовжуватиме працювати з останньою відомою конфігурацією, доки не буде відновлено підключення до хмари.

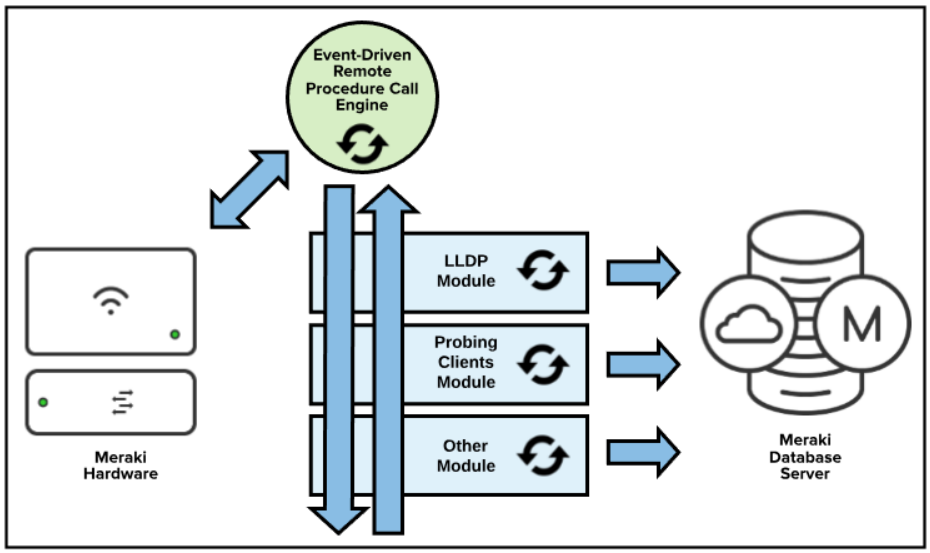


Рисунок 1.4 – Механізм Meraki Device-to-Cloud Communications

Процес спілкування. Якщо пристрій перебуває в автономному режимі, він продовжуватиме спроби підключитися до хмари Meraki, доки не встановить з'єднання. Коли пристрій підключається до мережі, він автоматично отримує останні налаштування конфігурації з хмари Meraki. Якщо в конфігурацію пристрою вносяться зміни, коли пристрій перебуває в режимі онлайн, пристрій автоматично отримує й оновлює ці зміни. Зазвичай ці зміни стають доступними на пристрої за лічені секунди. Однак велика кількість змін може зайняти помітно більше часу, щоб досягти своїх пристроїв. Якщо користувач не вніс жодних змін у конфігурацію, пристрій продовжує періодично самостійно перевіряти наявність оновлень у своїй конфігурації.

Коли пристрій працює в мережі, він передаватиме аналітику пристрою та використання мережі назад у хмару Meraki. Аналітика інформаційної панелі на основі цієї інформації у формі графіків і діаграм регулярно оновлюється в хмарі Meraki та відображається на інформаційній панелі користувачів, коли вони переглядають цю інформацію.

Інформаційна панель Meraki — це сучасне веб-базоване рішення для конфігурації пристроїв і сервісів Meraki. Вона слугує візуальною альтернативою традиційним командним інтерфейсам, які часто використовуються для управління маршрутизаторами, комутаторами та пристроями безпеки. Завдяки інформаційній

панелі Meraki, всі мережеві пристрої об'єднуються в єдиному інтерфейсі, де користувачі можуть легко вносити зміни у зрозумілому та інтуїтивно зрозумілому форматі (див. рис. 1.5).

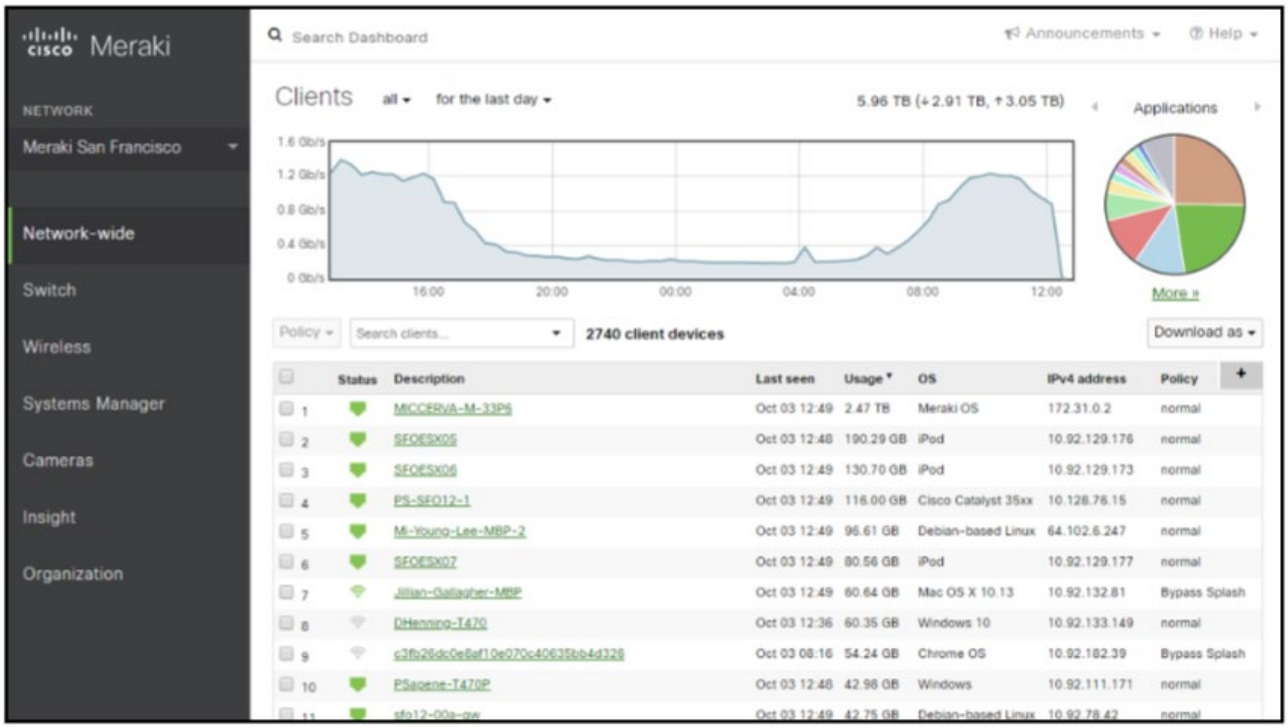


Рисунок 1.5 – Інформаційна панель Cisco Meraki

Крім спрощення управління пристроями, інформаційна панель Meraki також служить платформою для аналізу мережевої аналітики, налаштування мережевих політик і моніторингу користувачів. З цього інтерфейсу користувачі можуть переглядати відео з камер, управляти мобільними пристроями та комп'ютерами, налаштовувати правила контенту та контролювати вихідні з'єднання з одного місця.

Meraki API розширює функціональність інформаційної панелі, дозволяючи програмно управляти рішенням Meraki. Це RESTful API використовує HTTPS для передачі даних та JSON для серіалізації об'єктів, забезпечуючи більш глибокий рівень контролю, який може бути недоступний через інформаційну панель або вимагати більш деталізованого втручання. Відкритість API Meraki використовує

переваги хмарної платформи для створення більш продуктивних та потужних рішень, дозволяючи користувачам автоматизувати встановлення, управляти своїми мережами та розробляти кастомізовані додатки на базі інформаційної панелі Meraki (див. рис. 1.6).

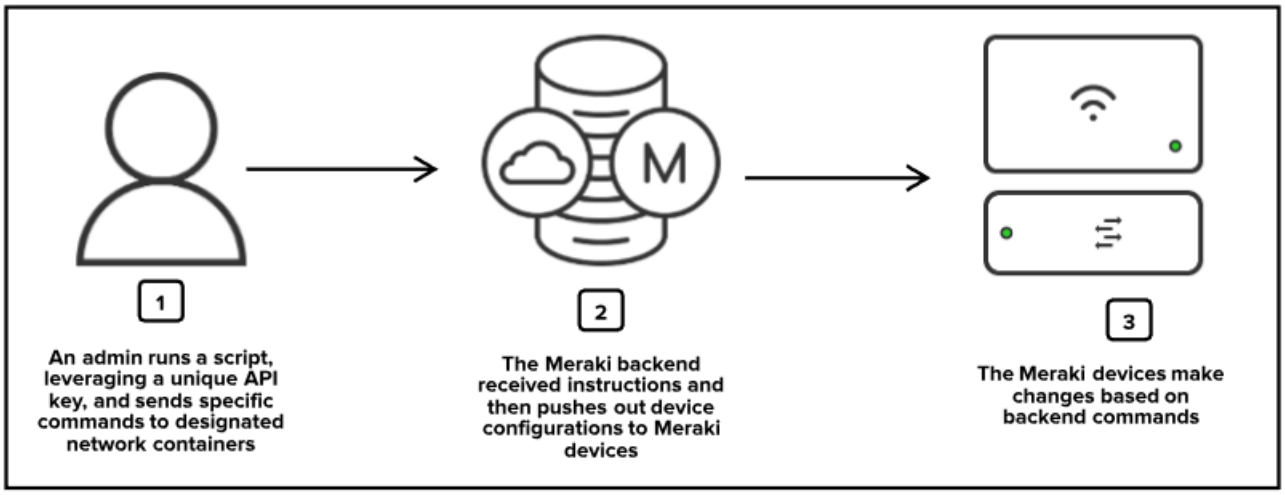


Рисунок 1.6 – Інтерфейс API Meraki

Ключі API прив’язані до конкретного облікового запису користувача через платформу Meraki. Якщо особа має адміністративний доступ до кількох організацій Meraki, один ключ може налаштувати та контролювати ці кілька організацій.

Надійність і доступність. Meraki підтримує архітектуру високої доступності різними способами, щоб забезпечити високу зручність обслуговування для наших клієнтів. Мережеві підключення через центри обробки даних мають високу пропускну здатність і високу стійкість. Спільні структури високої доступності забезпечують доступність даних у разі локального збою, а наша архітектура резервного копіювання центру обробки даних забезпечує постійну доступність даних керування клієнтами у разі катастрофічного збою (рис. 1.7). Ці резервні копії зберігаються в сторонніх хмарних службах зберігання. Ці сторонні служби також зберігають дані Meraki залежно від регіону, щоб забезпечити дотримання регіональних правил зберігання даних.

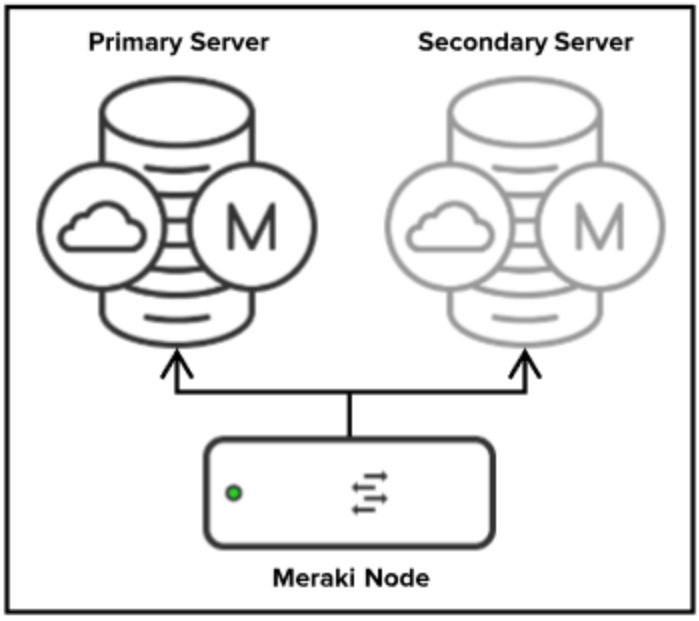


Рисунок 1.6 – Архітектура високої доступності

Meraki постійно контролює цілісність з’єднань, використовуючи численні високошвидкісні з’єднання зі своїх центрів обробки даних. Підключення до мережі Meraki виконує тести на доступність DNS, щоб визначити, що цілісність і центри обробки даних переключатимуться на вторинні канали у разі погіршення зв’язку.

Один пристрій підключається до кількох серверів Meraki одночасно, забезпечуючи актуальність усіх даних на випадок, якщо знадобиться перехід після відмови. Це вторинне підключення до сервера Meraki перевіряє цілісність конфігурації пристрою та історичні дані про використання мережі у разі збою сервера Meraki.

У разі збою сервера або втрати з’єднання підключення вузла може перейти на вторинний сервер. Після відновлення основного сервера з’єднання буде відновлено без помітного впливу на з’єднувальні вузли.

Висока доступність резервного копіювання центру обробки даних. Meraki зберігає активні дані керування клієнтами в основному та додатковому центрі обробки даних в одному регіоні. Ці центри обробки даних географічно розділені, щоб уникнути фізичних катастроф або збоїв, які потенційно можуть вплинути на той самий регіон. Дані, що зберігаються в цих центрах обробки

даних, синхронізуються в реальному часі. У разі збою в центрі обробки даних основний центр обробки даних переключиться на вторинний із збереженням останньої конфігурації (рис. 1.7).

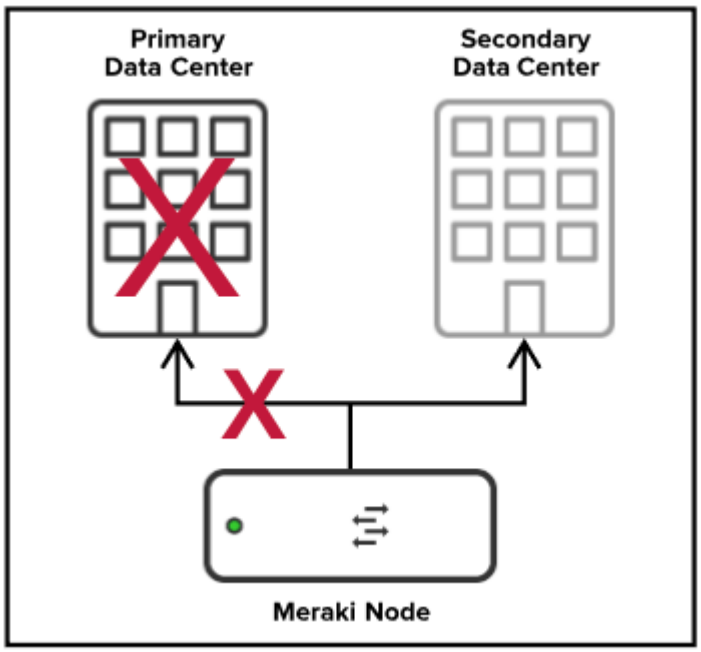


Рисунок 1.7 – Резервне копіювання центрів обробки даних

План аварійного відновлення. Зберігання даних керування клієнтами та надійність інформаційної панелі та API-служб є основними пріоритетами для Meraki. Щоб запобігти втраті даних у разі аварії, Meraki має кілька основних точок резервування. Кожен центр обробки даних Meraki об’єднується в пару з іншим центром обробки даних у тому ж регіоні. Якщо центр обробки даних повністю знищено, резервні копії можна створити за кілька хвилин в іншому центрі обробки даних у регіоні. Далі, якщо це вплине на обидва центри обробки даних, для відновлення даних можна використовувати нічні резервні копії, розміщені в двох різних хмарних службах зберігання сторонніх розробників, кожна з яких має власне резервне фізичне сховище.

1.2 Компоненти архітектури Cisco Meraki

Хмарне управління:

- Dashboard: Meraki Dashboard є веб-базованим інтерфейсом, який дозволяє користувачам легко налаштовувати та моніторити всю мережеву інфраструктуру, включаючи безпроводові мережі, комутатори, маршрутизатори безпеки та камери спостереження.

- Автоматичне оновлення: Система автоматично оновлюється, забезпечуючи новітні функції безпеки та продуктивності без потреби в ручному втручанні.

Компоненти мережі:

- Безпроводові точки доступу (APs): Meraki APs надають потужні і легко керовані безпроводові рішення для будь-якої організації.

- Комутатори: Комутатори Meraki забезпечують високу продуктивність і глибоку інтеграцію з безпроводовими рішеннями та безпекою.

- Маршрутизатори безпеки: Ці пристрої включають в себе файрволи, VPN-шлюзи, інструменти запобігання вторгненням та інші функції безпеки.

Аналітика та оптимізація:

- Traffic Shaping і QoS: Meraki дозволяє оптимізувати використання мережевих ресурсів за допомогою налаштувань Traffic Shaping та Quality of Service.

- Мережева аналітика: Інтегровані інструменти для аналітики надають глибокі відомості про використання мережі, здоров'я пристроїв і поведінку користувачів.

Приклади використання Cisco Meraki:

Освітні заклади: Школи та університети використовують Cisco Meraki для створення безпечних і легко керованих Wi-Fi мереж, які можуть обслуговувати тисячі студентів і викладачів.

Роздрібна торгівля: Торговельні мережі імплементують рішення Meraki для забезпечення Wi-Fi доступу клієнтам, а також для збору аналітичних даних про

поведінку покупців у магазинах.

Готельний бізнес: Готелі використовують Meraki для надання високоякісного інтернет-зв'язку своїм гостям і керування внутрішніми системами безпеки через одну платформу.

Великі підприємства: Корпорації інтегрують Meraki для керування своїми глобальними мережевими ресурсами, забезпечуючи високу доступність і безпеку корпоративних даних.

Завдяки централізованому управлінню, високій масштабованості, вбудованим функціям безпеки та розширеним аналітичним можливостям, Cisco Meraki є відмінним вибором для організацій, які шукають надійне, ефективне і легко кероване мережеве рішення.

Кожен пристрій Meraki, включаючи точки доступу, безпроводові комутатори Ethernet і пристрої безпеки, підключається через Інтернет до центру обробки даних Meraki, який керує платформою керування хмарою Meraki. Це з’єднання, захищене SSL, не лише використовує власний протокол, який забезпечує доступність і контроль у реальному часі, але також використовує мінімальну пропускну здатність даних (зазвичай 1 кбіт або менше).

Замість традиційної конфігурації мережі на основі командного рядка Meraki надає багатофункціональну веб-панель для доступу та керування десятками тисяч пристроїв Meraki по всьому світу. Ці інструменти призначені для масштабування великих розподілених мереж, зміни політик, оновлення прошивки, розгортання нових гілок тощо. Вони прості та зручні незалежно від розміру мережі та її розташування. Протоколи Meraki в режимі реального часу поєднують миттєве керування додатками з легкістю контролю та централізацією хмарного керування.

Кожен пристрій Meraki розроблений для хмарного керування. Це означає, що пристрої Meraki мають достатньо пам’яті та ресурсів процесора для своєчасної обробки пакетів, QoS, рівня безпеки 3-7, шифрування без додаткового навантаження на мережу. Таким чином, мережевий трафік не проходить через хмарне середовище, а функції керування даними з хмарного середовища надаються лише «на шляху». Ця архітектура дозволяє горизонтальне

масштабування та розширення мережі шляхом простого додавання додаткових кінцевих точок, не турбуючись про вузькі місця в центрі мережі. Крім того, тестування дизайну центру обробки даних Meraki продемонструвало здатність підтримувати десятки тисяч кінцевих точок одночасно.

Точки доступу Cisco Meraki складаються з компонентів найвищої якості та забезпечують безперебійну роботу (див. рис. 1.8). Завдяки Meraki користувачі можуть миттєво підключатися до мережі, яка має широкий радіус дії та підтримує велику кількість одночасних користувачів, з мінімальною потребою звертатися до служби підтримки.

Рисунок 1.8 - Точка доступу виробника Cisco Meraki

Точки доступу Meraki підтримують передові стандарти Wi-Fi 802.11n та 802.11ac, включаючи високоефективні антени, які забезпечують збільшення частоти прийому сигналів без зменшення радіусу покриття.

Переваги Cisco Meraki у порівнянні з альтернативними рішеннями на ринку включають:

- Ефективний процесор для перевірки та фільтрації мережевих пакетів;

- Завдяки використанню високошвидкісної пам'яті пристрій можна швидко налаштувати віддалено;

- Розширене використання радіочастотних діапазонів для кращої продуктивності;

- Підтримується метод MIMO для передачі сигналів через кілька антен одночасно.

- Централізоване управління: Керування всією мережею через єдиний веб-інтерфейс спрощує адміністрацію і знижує загальні витрати на управління.

- Швидке розгортання: Інфраструктуру можна швидко розгортати без необхідності в складних налаштуваннях, оскільки більшість конфігурацій та оновлень може бути здійснено дистанційно через хмарний дашборд.

Точки доступу Meraki надають розширену статистику використання мережі, надаючи вам більше гнучкості в управлінні налаштуваннями пристрою.

Інформаційні панелі Cisco Meraki відображають інформацію про користувачів мережі, їхні пристрої та програми. Завдяки такій багатій аналітиці адміністратори можуть швидко налаштувати контроль доступу та політику використання додатків, щоб не лише підвищити задоволеність користувачів, але й покращити безпеку мережі.

Універсальне, але інтуїтивно зрозуміле керування мережею за допомогою хмарних служб дозволяє вам відмовитися від високої вартості та складності керування наземними безпроводовими пристроями. Це єдине рішення на ринку, яке дозволяє керувати вбудованими мережами, проводовими та безпроводовими пристроями, підключеними до цих мереж, з одного екрана.

Аналіз на місці. CMX відображає статистику використання мережі в режимі реального часу, щоб допомогти підвищити задоволеність користувачів на місці. Платформа вбудована в точки доступу Meraki і не вимагає додаткових витрат або зусиль для налаштування. Зібрані дані синхронізуються з хмарним середовищем Cisco Meraki, що дає змогу зрозуміти тенденції трафіку користувачів, час безвідмовної роботи мережі та лояльність клієнтів у формі співвідношення нових користувачів до звичайних користувачів. CMX допоможе вам порівняти активність у мережі в різних місцях і під час різних рекламних кампаній, визначаючи ефективність ваших маркетингових кампаній на основі того, як довго відвідувачі залишаються в зоні покриття вашої мережі або як часто вони повторюють відвідування ваших місць. Панель також дозволяє переглянути дані

за певний день або побачити певні тенденції за місяць. А доступ до веб-інтерфейсу можна отримати з будь-якого інтернет-пристрою.

Завдяки потужним інструментам керування Cisco Meraki спрощує повсякденні завдання мережевих адміністраторів [4]:

- Додайте додаткові безпроводові мережі за лічені хвилини за допомогою повністю автоматизованого керування послугами зв'язку;

- Спрощене управління складними мережами в мінливих умовах за рахунок автоматичного налаштування радіочастот;

- Керуйте шириною каналу та блокуйте доступ до додатків двома кліками для додаткової зручності користувача;

- Налаштуйте програми, які використовують вбудовані служби платформи для підключення мобільних пристроїв до мережі.

В архітектурі Cisco Meraki мобільність є одним із головних факторів. Мобільна інформаційна панель Meraki, доступна для iOS і Android, ідеально підходить для керування мережею в дорозі.

Монітор:

- Контролювати стан і безпеку безпроводових і проводових мереж;

- Переглядайте стан мережі та споживання трафіку в реальному часі;

- Отримувати push-повідомлення у разі збою мережі.

Швидке сканування:

- Скануйте штрих-коди точок доступу, щоб швидко додати їх до мережі;

- Сфотографувати розташування точки доступу;

- Встановіть розташування точки доступу за допомогою GPS.

дистанційна діагностика:

- Перевірте підключення за допомогою інструментів реального часу;

- Віддалено вимірювати та аналізувати продуктивність мережі;

- Перезавантажте пристрій без залучення персоналу на місці.

Оновлення точок доступу через Інтернет постійно розширює їх функціональні можливості, що збільшує вартість вашої інвестиції. Вони повністю відповідають сучасним стандартам та сумісні з новітніми типами пристроїв та

програмними профілями. Також з'являються нові інструменти для візуалізації даних, аналізу та діагностики, доступні на інформаційних панелях.

Особливості точки доступу:

- Дозволяти або забороняти трафік рівня 3 для певних вузлів на певних портах TCP і UDP;

- Рівень 7 забороняє наступні типи трафіку (блоги, електронна пошта, обмін файлами, ігрові сервіси, новини, соціальні мережі тощо);

- Обмежте канали клієнтів (низхідні, вгорі, усі);

- Обмежені канали клієнтів (низхідні, висхідні, усі);

- Обмеження каналів для певних програм.

1.3 Апаратне забезпечення Cisco Meraki

Meraki MX доступний у 8 моделях проводових і безпроводових мережевих шлюзів. Вони відрізняються за технічними характеристиками та кількістю клієнтів, які обслуговують, але мають спільну рису – вбудовану систему безпеки (елементи якої зазначені вище), а також надійну апаратну частину. Візьмемо для прикладу модель MH400 (рис. 1.9) і розглянемо їх внутрішню будову. Існує жорсткий диск великої ємності для кешування, центральний процесор, який забезпечує багаторівневий аналіз трафіку та інші функції, оперативна пам’ять для роботи системи фільтрації вмісту та кілька мережевих пристроїв та інших пристроїв (4G модеми) мережевий інтерфейс. Крім того, кожен пристрій оснащений засобами шифрування та безпеки, які захищають передачу даних і забезпечують конфіденційність користувацької інформації.

Малі шлюзи. MX64 — це пристрій початкового рівня, призначений для підключення 50 клієнтів. Він має пропускну здатність брандмауера 250 Мбіт/с і VPN 85-100 Мбіт/с. Шлюз має п'ять гігабітних портів і може підключати USB 3G/4G модеми. Подібна модель MX64W має ті ж функції, але додатково постачається з модулем WiFi 802.11ac (рис. 1.10).

Модель MX65 має схожі характеристики, але кількість гігабітних портів

збільшено до 12, два з яких підтримують технологію Power over Ethernet (PoE) – можливість передачі живлення по витій парі. MX65W також оснащений модулем WiFi 802.11ac.

Рисунок 1.9 - Модель MX400

Середні шлюзи (рис. 1.11). Ці шлюзи відрізняються від менших шлюзів не лише підвищеною пропускною спроможністю та розміром, а й підтримкою топології типу «зірка» (концентратор і спиця), у якій вони діють як центральний вузол (концентратор). Модель MX84 має пропускну здатність брандмауера 500 Мбіт/с і VPN 200-250 Мбіт/с і розрахована на підключення до 200 клієнтів. Має 10 гігабітних портів, два модулі SFP і можливість підключення USB-модему. Як концентратор, MX84 може підключати до 100 периферійних точок. Ця модель також має мережеве кешування. До шлюзу MX100 можуть підключитися 500 клієнтів. Його пропускна здатність брандмауера становить 750 Мбіт/с, а пропускна здатність VPN — від 350 до 500 Мбіт/с. Є дев'ять гігабітних портів, два модулі SFP і можливість підключення USB-модему. Як концентратор він може приймати підключення від 250 пристроїв. Також є мережеве кешування.

Великі шлюзи. Окрім високої пропускної здатності, однією з головних особливостей найсучасніших моделей MX є можливість підключення додаткових модулів. Тому ви можете розширити шлюз за потреби. Пристрій MH250 розрахований на підключення до 2000 клієнтів. Його пропускна здатність брандмауера становить 1 Гбіт/с, а його VPN — від 900 Мбіт/с до 1 Гбіт/с. Кількість гігабітних портів до 20, а також до 16 SFP і до 4 SFP+. Також можна підключити USB 3G/4G модем. Як хаб ця модель може підключати до 1000

пристроїв, має систему мережевого кешування та резервне джерело живлення. Кількість портів у моделі MX450 така ж, як і в попередній моделі. Але до нього можуть підключитися 10 000 клієнтів, а як хаб він може вмістити до 5 000 пристроїв. Пропускна здатність брандмауера - 1 Гбіт/с, VPN - від 900 Мбіт/с до 1 Гбіт/с. Можливе підключення USB-модемів, мережевого кешу та додаткових джерел живлення.

Рисунок 1.10 - Моделі MX64 та MX64W

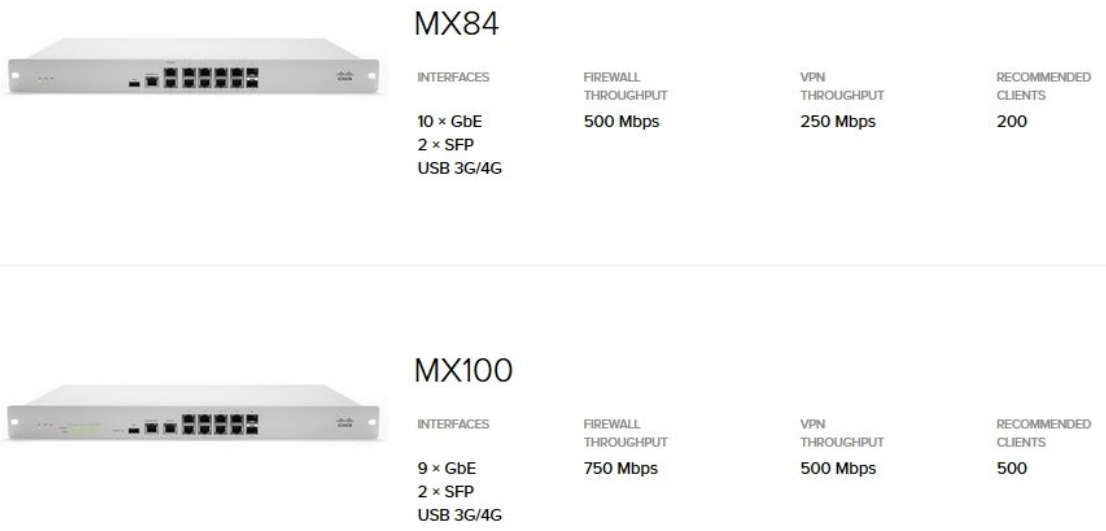


Рисунок 1.11 - Моделі MX84 і MX100

Точки доступу Meraki мають 13 внутрішніх і зовнішніх точок доступу. Вони відрізняються за технічними характеристиками, можливостями використання, але використовують однакові частоти та технології, а також надійне обладнання. На прикладі моделі AP MR32 (рис. 1.12) розглянуто їх внутрішні компоненти. Він має 2 радіомодулі 5 ГГц 802.11a/n/ac і 2,4 ГГц 802.11b/g/n, спеціальну радіостанцію, яка забезпечує безпеку та оптимізує радіозв'язок за допомогою інтегрованого аналізу спектру.

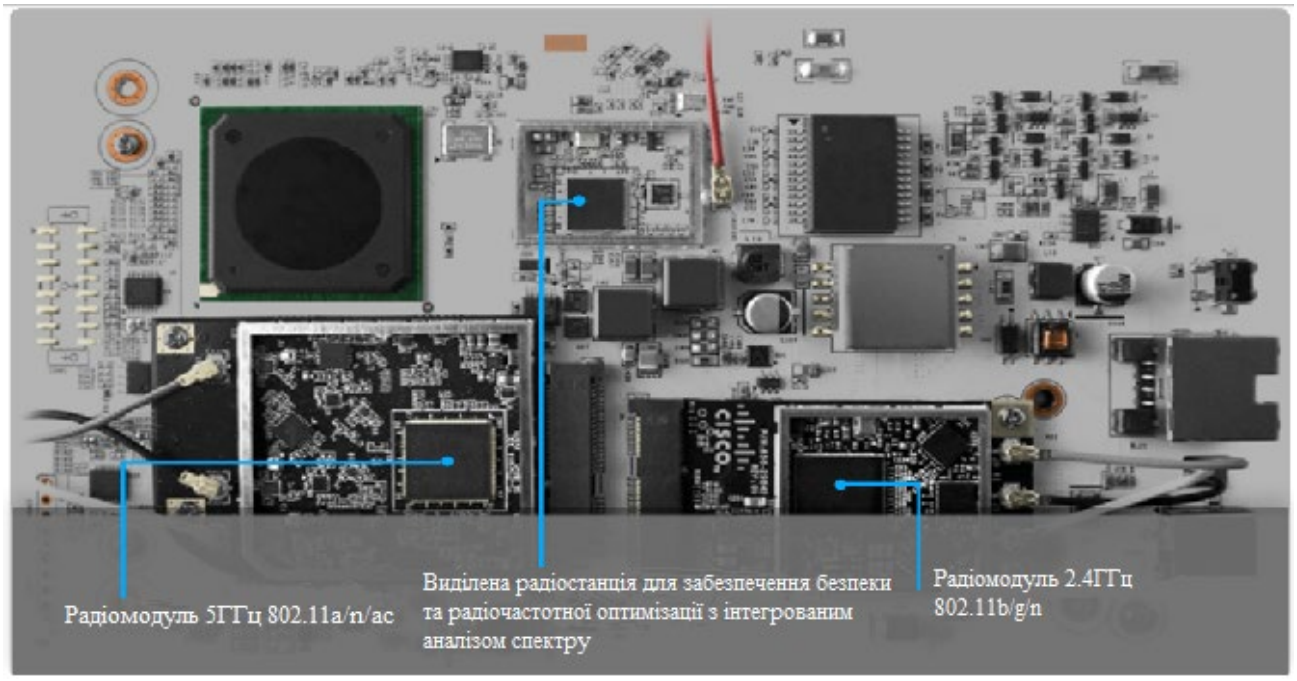


Рисунок 1.12 - Модель MR32 AP

Кожна точка доступу Meraki безперервно й автоматично контролює своє середовище, щоб максимізувати продуктивність WiFi. Вимірюючи використання каналу, силу сигналу та пропускну здатність точки доступу, Meraki автоматично оптимізує продуктивність окремих точок доступу та максимізує загальну продуктивність системи. Точки доступу Cisco Meraki були розгорнуті та протестовані в найвимогливіших середовищах, підтримуючи більше ніж 100 користувачів на пристрій і спільно надаючи трафік 100 Мбіт/с на тисячі пристроїв. Усуваючи традиційні контролери, Meraki також усуває вузькі місця

продуктивності, які часто стикаються з безпроводовими мережами високої щільності. Безпроводові канали, вихідна потужність точки доступу та параметри підключення клієнта автоматично адаптуються до змін робочих характеристик і умов перешкод, усуваючи необхідність ручного налаштування десятків окремих параметрів.

Внутрішня точка доступу. MR20 AP — це безпроводовий пристрій початкового рівня, який підходить для розгортання малого бізнесу та SOHO (маленький офіс, домашній офіс). Основа для розгортання безпроводового зв'язку з дуже низькою щільністю. Він підтримує дві частоти (2,4 ГГц і 5 ГГц) з максимальною пропускною здатністю 1,3 Гбіт/с. Має антену 2x2 MIMO, гігабітний порт.

Точка доступу MR32 - схожа на MR20 AP. Він більш широко використовується в кампусах з високою щільністю. Поставляється з вбудованою системою виявлення та запобігання вторгненням і Bluetooth.

MR30H AP — це потужніша точка доступу, призначена для розгортання в готельних або гуртожиткових номерах. Він має всі функції точки доступу MR20, але також оснащений інтегрованою системою виявлення та запобігання вторгненням, Bluetooth, чотирма додатковими гігабітними портами, Один з них підтримує технологію PoE.

MR34 AP – має вищу швидкість 1,75 Гбіт/с, оснащений трьома потоками MIMO та потребує PoE+ для повної функціональності.

MR42 AP - Відмінності від MR34 збільшенням пропускної здатності до 1,9 Гбіт/с. Подібна модель MR42E AP має ті самі функції, але постачається з 5 додатковими знімними антенами.

MR45 AP — це потужніша точка доступу з технологією WiFi 6, яка підтримує OFDMA — множинний доступ з ортогональним частотним розподілом каналів. Ця функція дозволяє покращити передачу даних у безпроводових мережах із високою щільністю пристроїв. При цьому зменшується затримка доставки пакетів для кожного користувача. Пропускна здатність - 3,5 Гбіт/с. Він має ширину каналу до 160 МГц, має мультигігабітні порти 2,5 Гбіт/с і

поставляється з 4 потоками MIMO.

MR52 AP — пропускна здатність 2,5 Гбіт/с із 4 потоками MIMO, двома гігабітними портами, інтегрованою системою виявлення та запобігання вторгненням і шириною каналу 160 МГц.

MR53 AP — це високопродуктивна точка доступу для кампусів з високою щільністю з кількома гігабітними та одним гігабітним портами зі швидкістю до 2,5 Гбіт/с. Існує також модель, подібна до цієї MR53E, яка постачається з додатковими 6 знімними антенами.

MR55 AP є найпотужнішою наявною моделлю. Точка доступу працює на основі технології WiFi 6 і має 8 потоків MIMO та мультигігабітні порти з пропускною здатністю 5 Гбіт/с.

Зовнішня точка доступу. MR70 — це базова зовнішня точка доступу, яку можна розгортати при дуже низькій щільності. Працює на двох діапазонах частот, з двома потоками MIMO, пропускна здатність - 1,3 Гбіт/с. Має гігабітний порт і вбудовану багатонаправлену антену. Підтримує функцію PoE, водонепроникний і пилонепроникний. MR74 є вдосконаленою версією MR70. Він має всі функції MR70, але поставляється з 4 додатковими антенами, що покращує якість сигналу та радіус дії, а також робить його більш стійким до погодних умов. Він також включає інтегровану систему виявлення та запобігання вторгненням і Bluetooth.

MR84 є найпотужнішою зовнішньою точкою доступу, доступною в архітектурі Meraki. Розроблено для жорстких радіочастот і середовищ із високою щільністю. Він має інтегровану систему виявлення та запобігання вторгненням і Bluetooth, 4 потоки MIMO, 1 мультигігабітний порт 2,5 Гбіт/с і 1 гігабітний порт, 4 антени посилення сигналу, можливість PoE+. Він водонепроникний, пилонепроникний і дуже стійкий до впливу елементів.

Отже, система Cisco Meraki легко масштабується від невеликих офісів до великих підприємств, забезпечуючи однаково високу ефективність та централізоване управління незалежно від розміру мережі, інтегровані засоби безпеки, такі як файрволи, функції протидії вторгненням та VPN, забезпечують захист мережі на різних рівнях.

2 РОЗГОРТАННЯ АРХІТЕКТУРИ CISCO MERAKI

2.1 Налаштування точок доступу

Класичні рішення для контролерів AP і новинки від Cisco, одним з яких є Cisco Meraki. Ми зробили вибір на користь Cisco Meraki, оскільки всі продукти цього сімейства організовані таким чином, щоб спростити завдання сучасних мережевих пристроїв і програм.

Щоб розширити інфраструктуру WLAN, ми проаналізували список продуктів Cisco Meraki та замовили чотири точки доступу MR32 AP і дорожчу точку доступу MR34 (рис. 2.1).

Рисунок 2.1 - Точки доступу MR34 AP

В Перейдіть на сторінку http://dashboard.meraki.com і увійдіть. Щоб заощадити час на встановлення точок доступу, вони вже встановлені й успішно оновлені, а кожній точці доступу присвоєно статичну IP-адресу. Щоб точка доступу працювала належним чином, її необхідно підключити до розетки

Ethernet. MR32 увімкнеться, і світлодіод стане помаранчевим, а потім зеленим протягом 30 секунд. Це означає, що жоден користувач ще не підключився до точки доступу. У цьому випадку буде транслюватися відкрита та незахищена безпроводова мережа з логіном Meraki. Пристрої Cisco Meraki автоматично підключаються до хмарного середовища за допомогою протоколу шифрування SSL, реєструються в мережі та завантажують конфігурацію. Після підключення до мережі за протоколом DHCP можна виконати основні налаштування (рис. 2.2) [5].

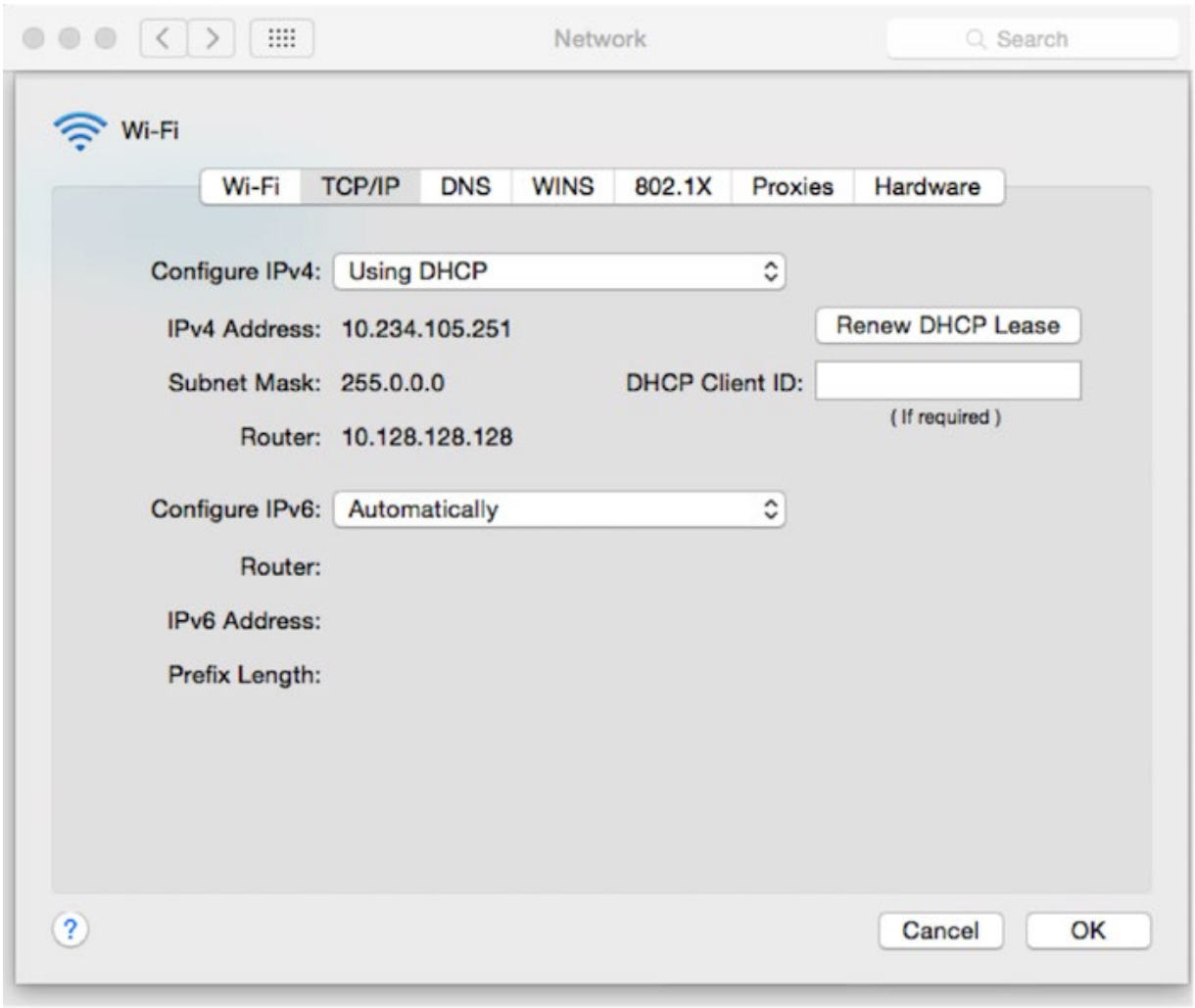


Рисунок 2.2 - Перегляд шлюзу за замовчуванням

У веб-інтерфейсі точки доступу можна встановити кілька налаштувань (VLAN, широкомовний канал Wi-Fi і живлення, а також проксі). Управління обладнанням Meraki здійснюється за допомогою хмарної панелі керування. Таким чином, пристрої Meraki повинні мати доступ до зовнішніх мереж за допомогою

наступних протоколів (рис. 2.3):

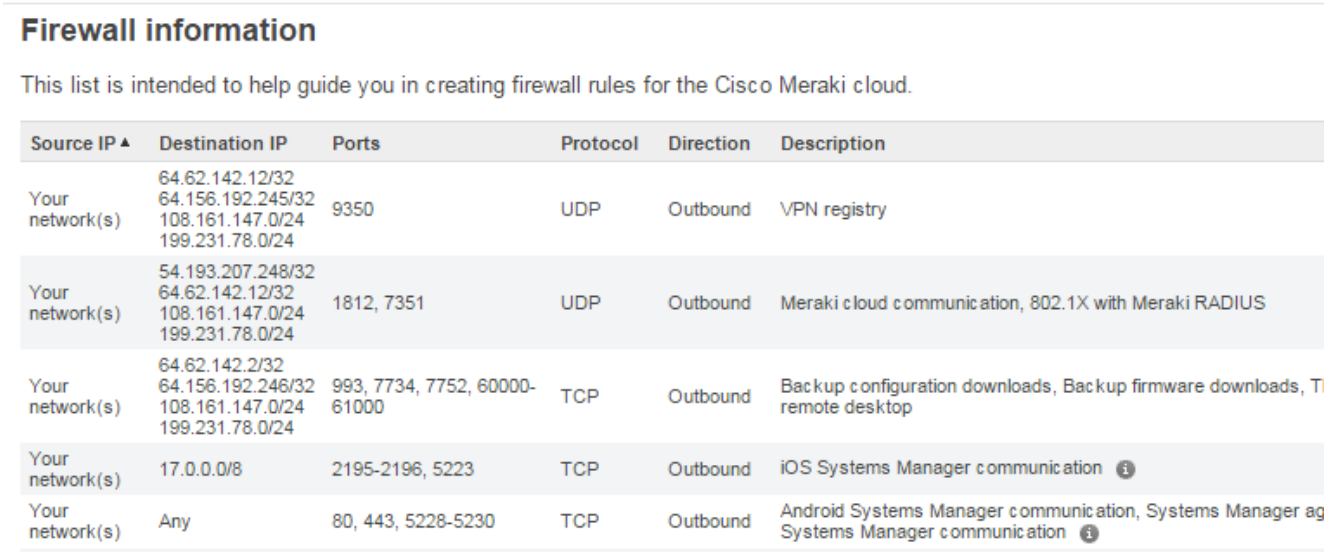
- протокол UDP, номер порту 9350, який використовується для VPN;

- протокол UDP, номери портів 1812, 7351, для зв’язку з хмарним середовищем Meraki та використання Meraki RADIUS;

- протокол TCP, номери портів 993, 7734, 7752, 60000-61000, використовується для завантаження резервної копії конфігурації та завантаження резервної копії програмного забезпечення;

- протокол TCP, номери портів 2195 - 2196, 5223, необхідні для зв'язку з системою управління на iOS;

- протокол TCP, номери портів 80, 443, 5228 - 5230, необхідні для зв'язку з системою управління Android.



Firewall information

This list is intended to help guide you in creating firewall rules for the Cisco Meraki cloud.

Source IP ▲	Destination IP	Ports	Protocol	Direction	Description
Your network(s)	64.62.142.12/32 64.156.192.245/32 108.161.147.0/24 199.231.78.0/24	9350	UDP	Outbound	VPN registry
Your network(s)	54.193.207.248/32 64.62.142.12/32 108.161.147.0/24 199.231.78.0/24	1812, 7351	UDP	Outbound	Meraki cloud communication, 802.1X with Meraki RADIUS
Your network(s)	64.62.142.2/32 64.156.192.246/32 108.161.147.0/24 199.231.78.0/24	993, 7734, 7752, 60000-61000	TCP	Outbound	Backup configuration downloads, Backup firmware downloads, T remote desktop
Your network(s)	17.0.0.0/8	2195-2196, 5223	TCP	Outbound	iOS Systems Manager communication
Your network(s)	Any	80, 443, 5228-5230	TCP	Outbound	Android Systems Manager communication, Systems Manager ag Systems Manager communication

Рисунок 2.3 - Необхідні протоколи для нормального функціоналу пристроїв

Щоб повною мірою скористатися всіма функціями веб-інтерфейсу Cisco Meraki Cloud Management, вам потрібно надати доступ за допомогою потоку, показаного вище (рисунок 2.4). Таким чином забезпечується повна видимість і контроль мережі через Інтернет. Немає необхідності постійно налаштовувати мережу у вашому офісі чи на підприємстві.

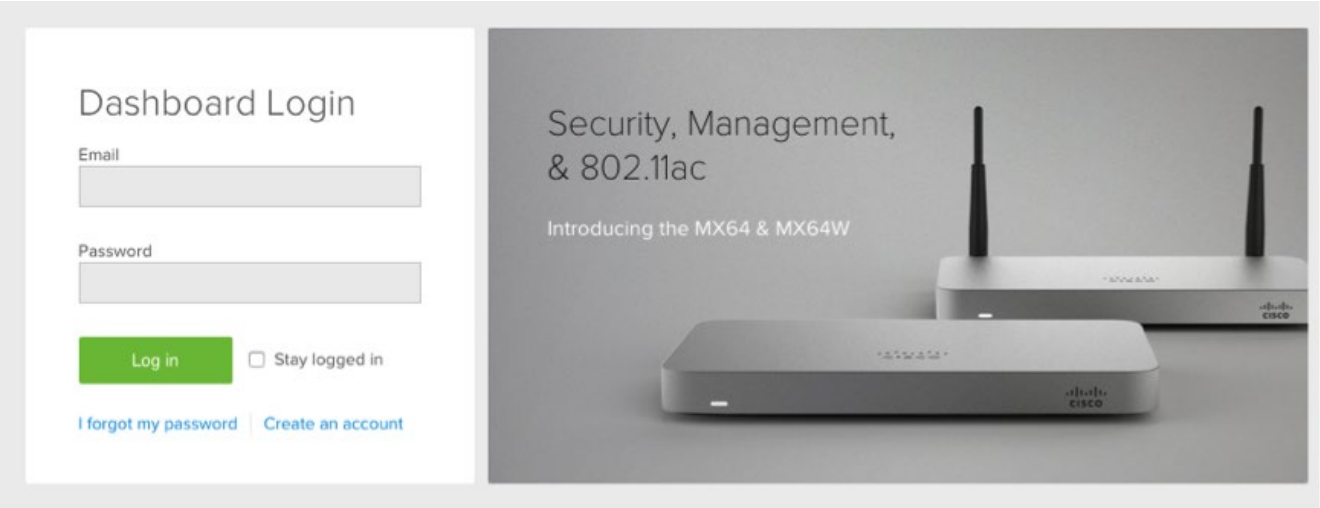


Рисунок 2.4 - Приклад веб-інтерфейсу Cisco Meraki cloud management

За замовчуванням точки доступу Cisco Meraki вже мають безпроводову інфраструктуру з певними параметрами. Це дуже зручна функція, оскільки вона значно спрощує початкове налаштування мережі в цілому. Це було не зовсім задовільним, тому було вирішено видалити існуючу інфраструктуру WLAN. У головному меню хмарного інтерфейсу видаліть усі точки доступу з тестової мережі WLAN, натиснувши кнопку «Видалити з мережі», щоб видалити точку доступу зі списку готових мереж (рис. 2.5).

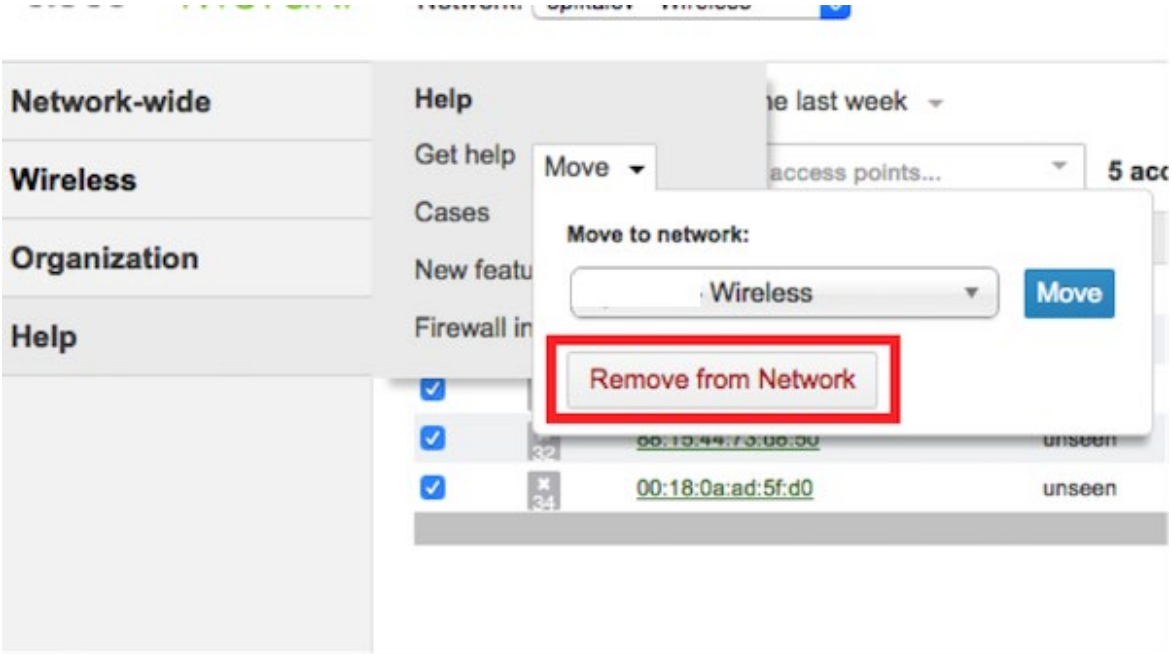


Рисунок 2.5 - Видалення точок доступу з мережі

Потім починають створювати все з нуля. Створити нову мережу не дуже складно. Створюючи мережу, ви вибираєте її ім’я, тип мережі, конфігурацію (ви можете використовувати стандартні параметри або скопіювати з існуючої мережі у файлі конфігурації Meraki) і додаєте пристрої до таблиці мереж. Для цього знадобиться номер замовлення Meraki або серійний номер для кожної точки доступу, який виглядатиме як Qxxx-xxxx-xxxx і розташований у нижній частині пристрою. Вам також знадобиться ліцензійний ключ підприємства, який ви повинні отримати електронною поштою. Ми створили мережу, назвавши тест мережі ISH, вибравши тип безпроводового з’єднання та додавши 5 точок доступу до таблиці (рис. 2.6). Далі ми переглядаємо план на карті та розміщуємо кожну точку доступу на карті, клацаючи та перетягуючи її в місце, де ми вирішуємо її встановити [6].

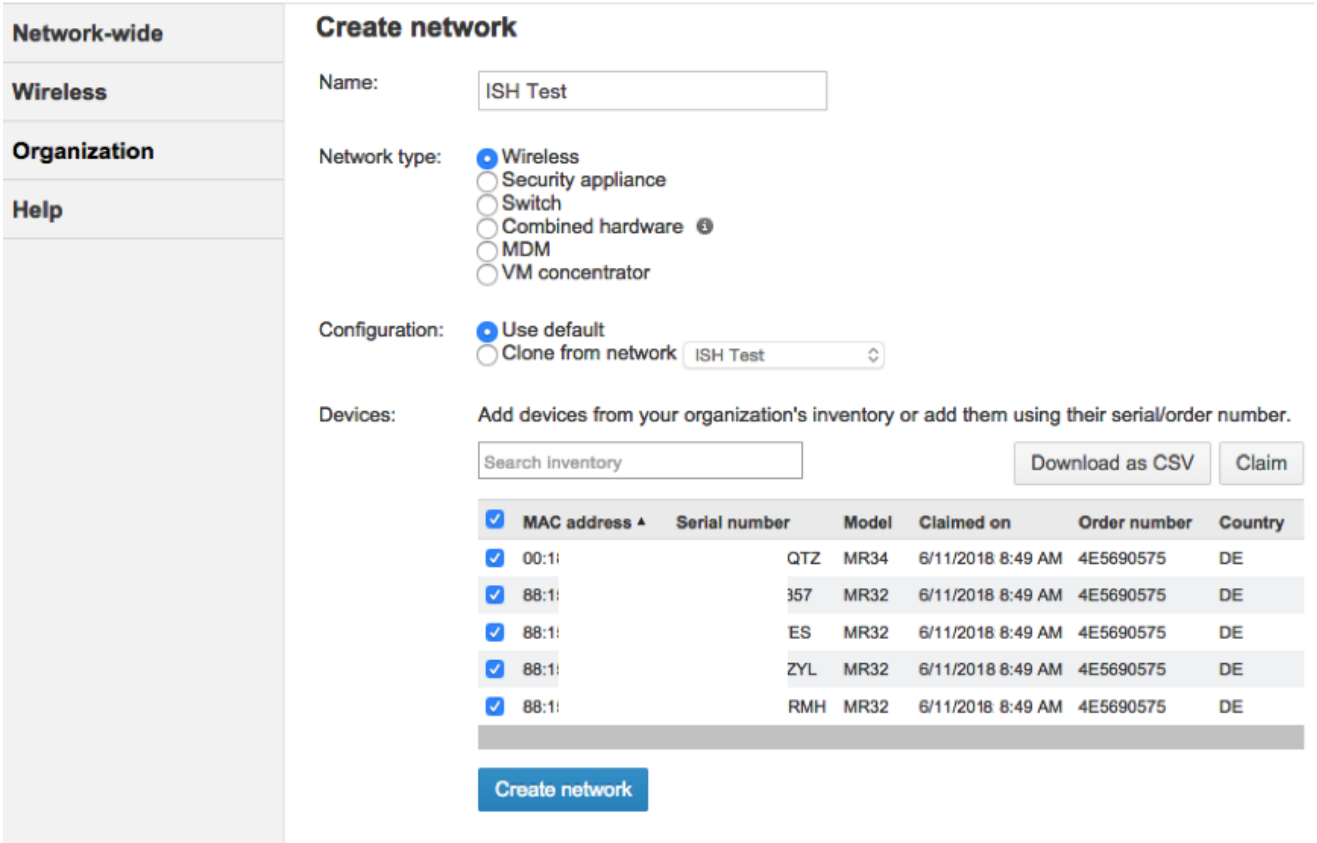


Рисунок 2.6 - Створення нової мережі

Точка доступу отримує нові налаштування протягом десятків секунд і починає роздавати SSID «ISH Test». Далі приступають до налаштування мережі.

Елементи налаштування включають наступні параметри (рис. 2.7):

– SSID. Безпроводова мережа може мати до 15 SSID;

- управління доступом;

- брандмауер і обмеження трафіку;

- спливаюча сторінка;

– наявність SSID;

- налаштування Bluetooth;

- встановити радіосигнал.

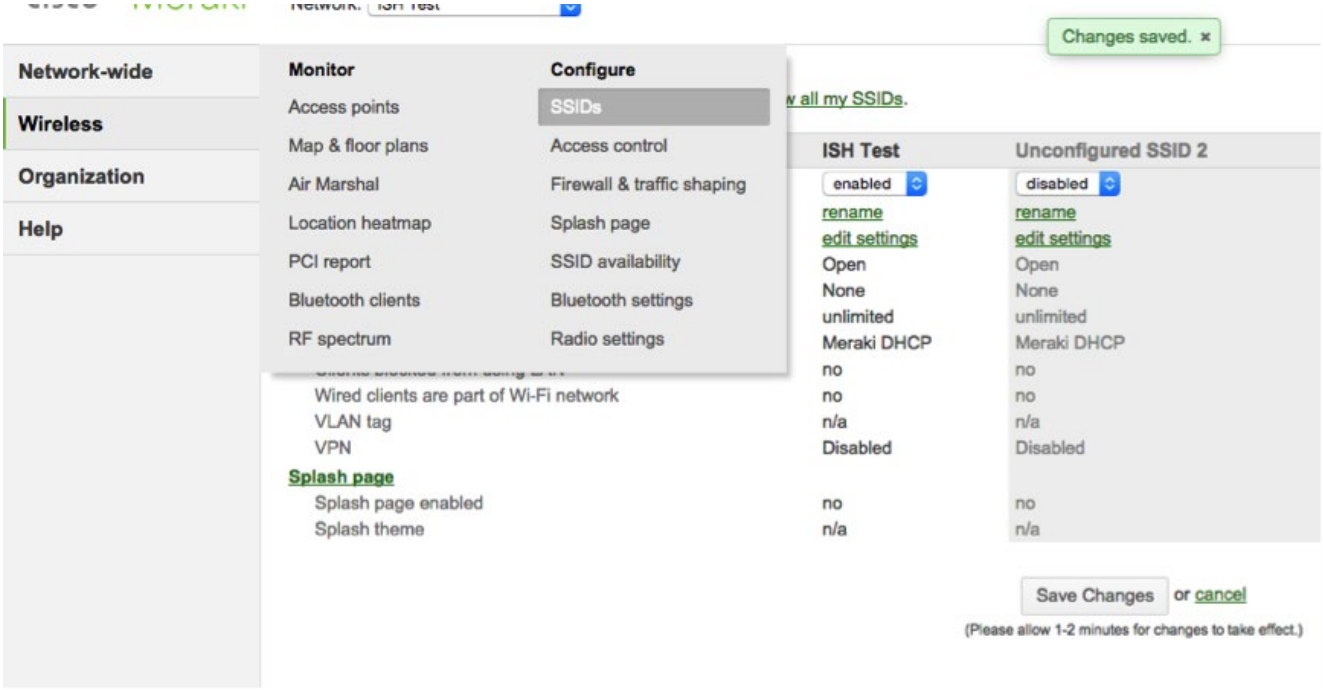


Рисунок 2.7 - Меню конфігурації у веб-інтерфейсі

– Наступне завдання — налаштувати шифрування та мережеві ключі. Після натискання «Редагувати налаштування» для першого SSID ми входимо до розділу його налаштувань. У цьому меню ви можете переглянути та налаштувати типи автентифікації, необхідні для належної роботи мережі. У Cisco Meraki існує велика кількість можливостей автентифікації (рис. 2.8).

– Параметри автентифікації:

– Доступ на основі таблиці MAC-адрес;

– WPA2-Enterprise може використовувати внутрішні сервери RADIUS і

сервери Meraki. У випадку з Meraki аутентифікація здійснюється за допомогою облікових даних, які потрібно використовувати для входу в панель керування мережею;

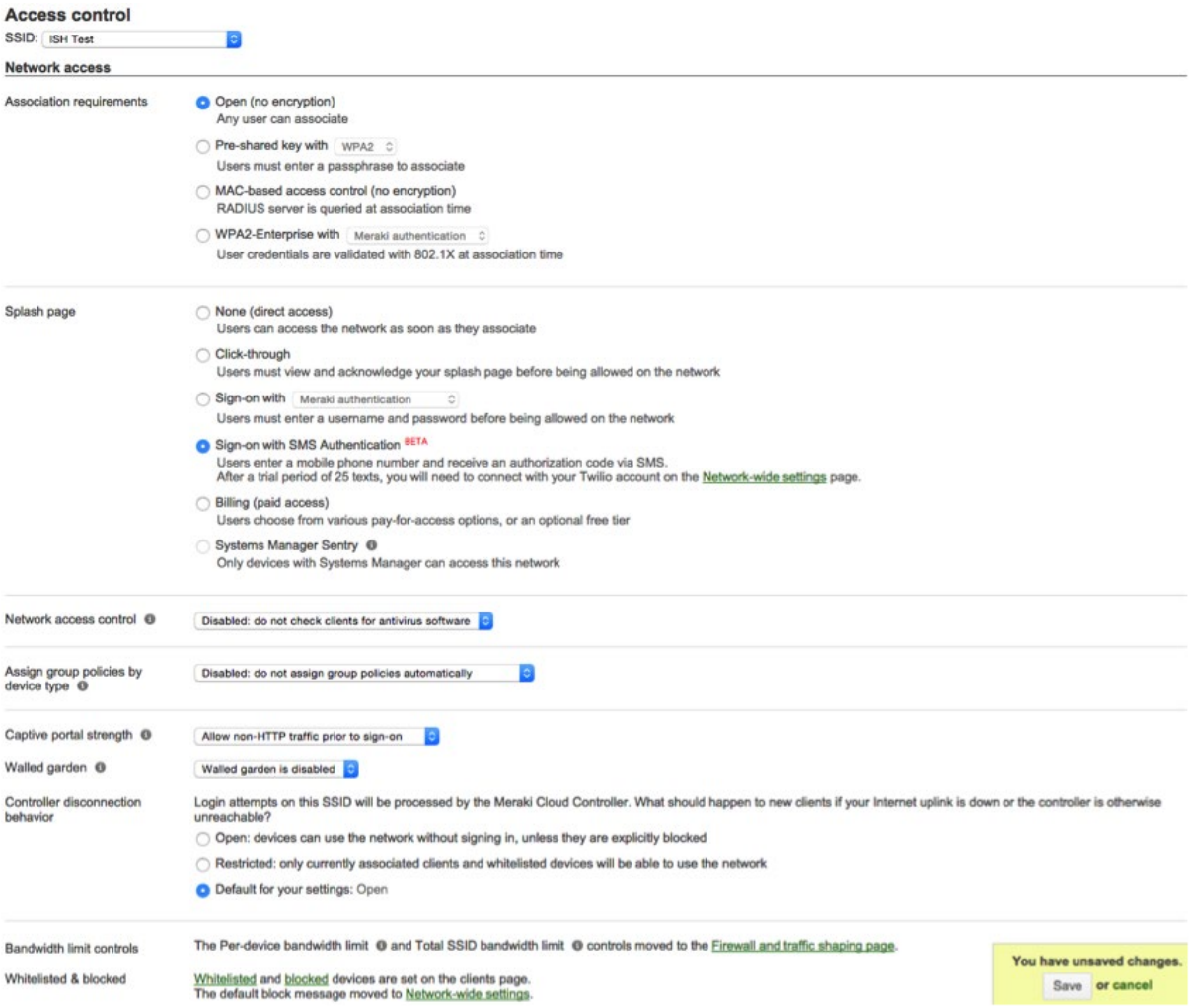


Рисунок 2.8 - Перелік способів аутентифікації

– крім цього можна вибрати тип шифрування WPA.

Далі йде параметр Splash page - сторінка, яка відображається після авторизації в мережі WIFI. Цей механізм часто використовується в публічних мережах – аеропортах, готелях, кафе тощо.

Перерахуємо по пунктах:

- пряме інтерв'ю;

- натискання – клієнти повинні натиснути кнопку на сторінці, наданій їм точкою доступу. Наприклад, його можна використовувати, щоб змусити користувачів прочитати та прийняти умови використання мережі;

- використовувати додаткову аутентифікацію (Meraki Server, RADIUS, LDAP, Active Directory, Facebook Wi-Fi, Google Authentication);

- автентифікація шляхом введення SMS-коду. Перші 15 повідомлень безкоштовні, потім потрібно зареєструватися на сервісі Twilio, придбати підписку та оплатити повідомлення.

Давайте розберемо варіанти автентифікації через Splash Page. Прямий доступ - все просто, сторінка не відображається, відразу заходимо в мережу. Клацніть Pass. Після підключення у вашому браузері з'явиться запит натиснути кнопку та підключитися до Інтернету (рис. 2.9).

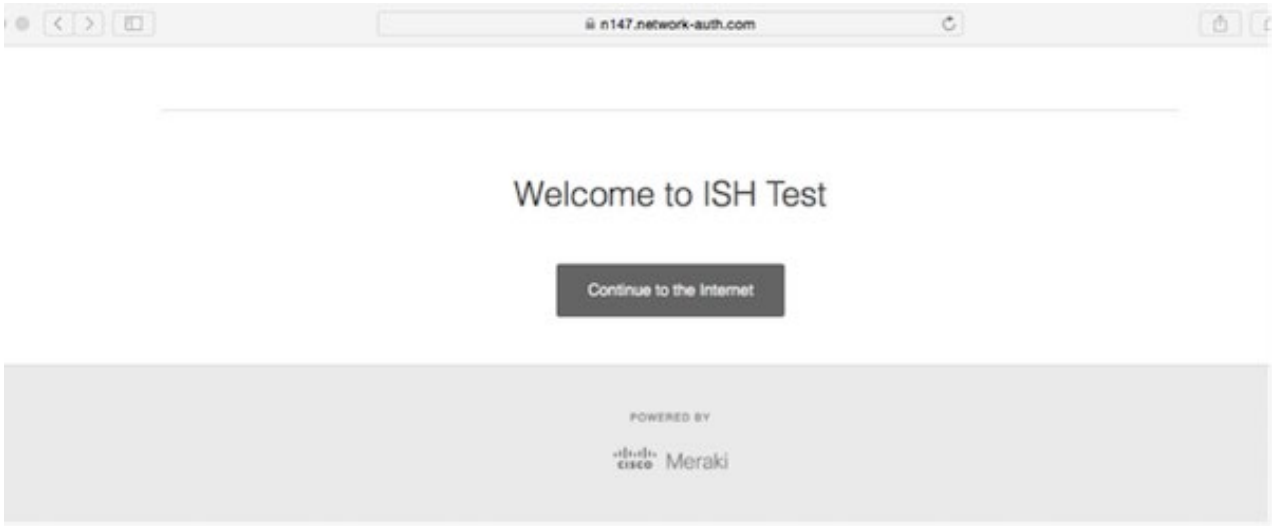


Рисунок 2.9 - Приклад використання Click through

Доступ в Інтернет з використанням додаткової аутентифікації. Ми налаштовуємо доступ до контролера домену та встановлюємо там правила підключення користувачів до Інтернету. Ми додали декілька логінів із різними дозволами на використання мережі та призначили різні паролі для кожного входу.

Щоб просто перевірити автентифікацію, ви можете натиснути кнопку «Перевірити». Одразу відкриється сторінка автентифікації користувача. Ввівши в AD логін і пароль будь-якого користувача, ми отримуємо доступ до мережі (рис. 2.10) [7].

Один з інших цікавих варіантів аутентифікації - через Facebook WiFi. Для того, щоб активувати аутентифікацію через Facebook WiFi, потрібно мати Local

Business Page організації. Зайшовши в налаштування Facebook WiFi, виставляємо check-in через Facebook і також вибирали підключення через пароль, який теж можемо встановити самостійно (рис. 2.11). Також можна вибрати час сесії користування користувача.

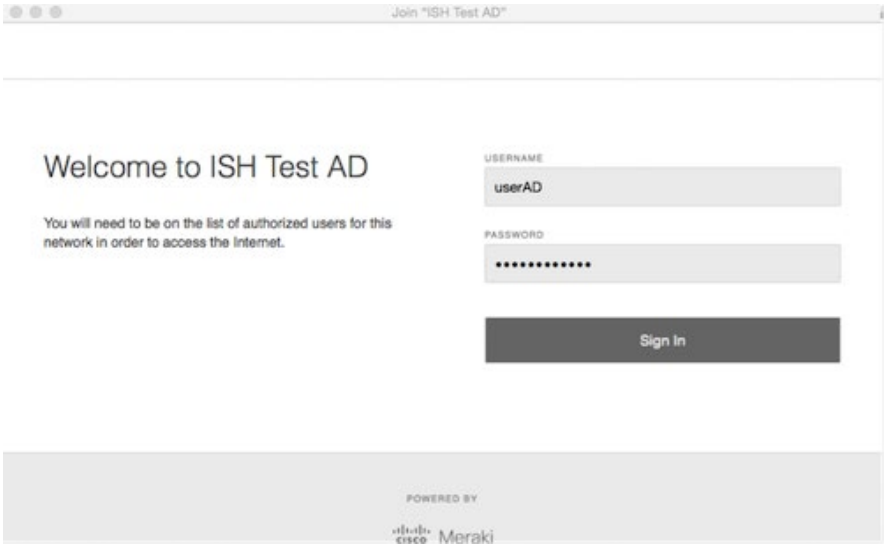


Рисунок 2.10 - Аутентифікація користувача через Active Directory

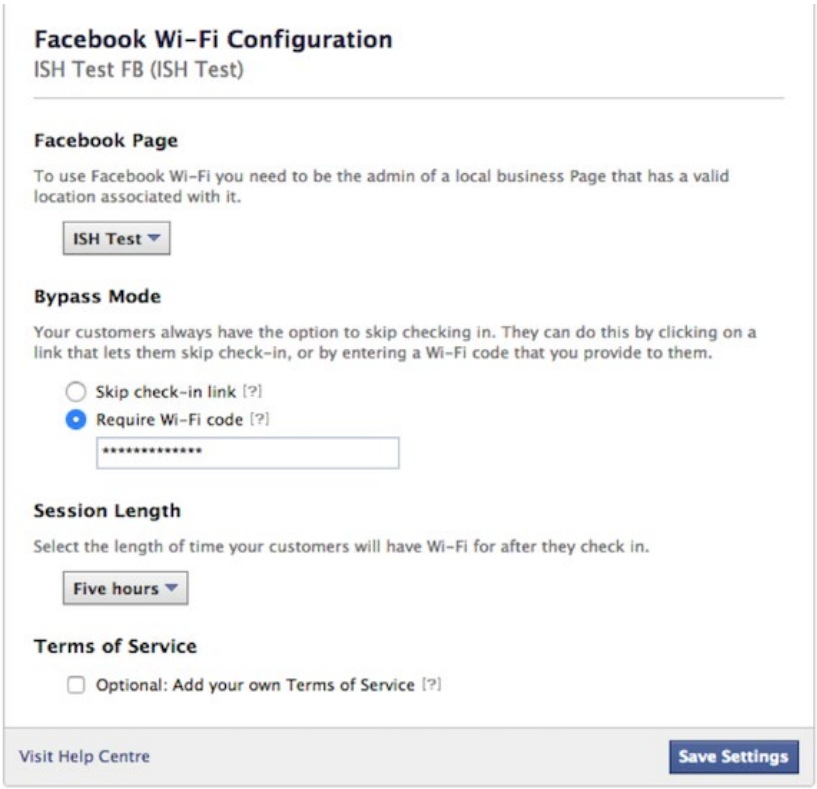


Рисунок 2.11 - Налаштування аутентифікації через Facebook WiFi

Підключившись до мережі одразу з'являється сторінка з аутентифікацією Facebook WiFi. Де користувач зможе вибрати як підключитися до мережі Інтернет, через Facebook чи використати спеціальний пароль, який присвоювали налаштуваннях. Вхід в Facebook забезпечує соціальну реєстрацію користувачів, які входять в точки доступу Meraki MR і пристрої безпеки MX. Можна використовувати свою сторінку Facebook в якості сторінки входу, яку користувач бачить при першому вході в вашу мережу. Потім користувачі можуть зареєструватися, використовуючи свої облікові дані Facebook, оновити свій статус і «лайкнути» сторінку Facebook.

Переваги використання Facebook WiFi [7]:

– забезпечте кращу взаємодію з користувачем через WiFi - вхід в систему через Wi-Fi є «соціальним», друзі можуть ділитися своїм місцеположенням і відзначати інших друзів, додавати фотографії;

– більше спілкуйтеся зі своїми кінцевими користувачами - збільшуйте трафік на своїй сторінці в Facebook, діліться пропозиціями та оголошеннями, спрощуйте для своїх клієнтів реєстрацію і збільшуйте популярність вашого бізнесу;

– підвищуйте впізнаваність свого бізнесу в Facebook - вхід в Facebook сприяє повторної реєстрації. Це означає, що ваш бізнес може збільшити число людей, з якими ви спілкуєтеся, а також кількість історій про ваш бренд в новинній стрічці;

– поглибшуйте аналітику в соціальних мережах - отримуйте уявлення про сукупні демографічні дані при реєстрації, залучуйте клієнтів, які реєструються за допомогою реклами на Facebook.

Також присутня аутентифікація по SMS. При підключенні до WiFi відкривається сторінка, де користувача просять ввести його номер телефону. Це ініціює відправлення SMS з кодом аутентифікації на номер користувача. Користувач вводить код і отримує доступ до мережі Інтернет.

2.2 Налаштування доступу до мережі

Також присутній платний доступ. Включивши опцію "Billing (paid access)", налаштували Billing plans. Дана функція дозволяє вибрати безкоштовний період на певний час використання мережі, валюту, якою буде здійснюватися оплата, налаштування правил оплати, типи платіжних засобів, можливість передоплати тощо.

Підключившись до мережі, одразу з'являється сторінка, де нам пропонують оплатити користування мережею або ж увійти вже через обліковий запис, який оплачений. Оплативши, користувач одразу отримує доступ до мережі Інтернет.

Ось і всі варіанти додаткової аутентифікації через Splash Page. Окремо варто відзначити, що є можливість обмежити доступ до мережі з певних платформ (Android, BlackBerry, Chrome OS, iPad, iPhone, iPod, MacOS, Windows, Windows Phone, B & N Nook, other OS), а також обмежити можливість використання одного і того ж облікового запису на декількох пристроях одночасно.

Для аутентифікації використали Meraki Radius. Для його використання під обліковим записом адміністратора треба завести користувачів, паролі для них, вказати їх email і встановити опцію, яка включає доступ користувачеві до SSID. Користувачі можуть отримувати свої облікові дані поштою автоматично.

Далі переходимо до налаштувань роутингу і трафіку. WLAN точки доступу Meraki підтримують 5 типів адресації (рис. 2.12) [8]:

– режим NAT. Користувачі будуть отримувати IP з діапазону 10.0.0.0/8, не зможуть контактувати між собою. У цьому режимі можна включити фільтрацію контента, яка може працювати в двох режимах: блокування матеріалів для дорослих або вказівки власного DNS, на який призначена функція блокування;

– режим мосту, клієнти працюють в підмережі, до якої підключена точка доступу. Подтримуються VLAN теги. Підтримується Bonjour переадресація та її вимкнення;

– роумінг третього рівня. Аналогічний режим мосту, але в цьому випадку клієнти при переході з одної точки доступу до іншої будуть зберегти свію IP-адресу (у випадку, якщо точки доступу працюють в одному списку). Поддерживаются VLAN теги. Підтримується Bonjour переадресація та її відключення;

– роумінг третього рівня з концентратором. Клієнти віходять в мережу через концентратор, який представляє собою окреме пристрій.

– VPN: тунельні дані до концентратора. Принцип той самий, що і в роумінгу третього рівня з концентратором, але дані будуть шифруватися і передаватися через шифроване VPN-підключення між точками доступу та концентраторами.

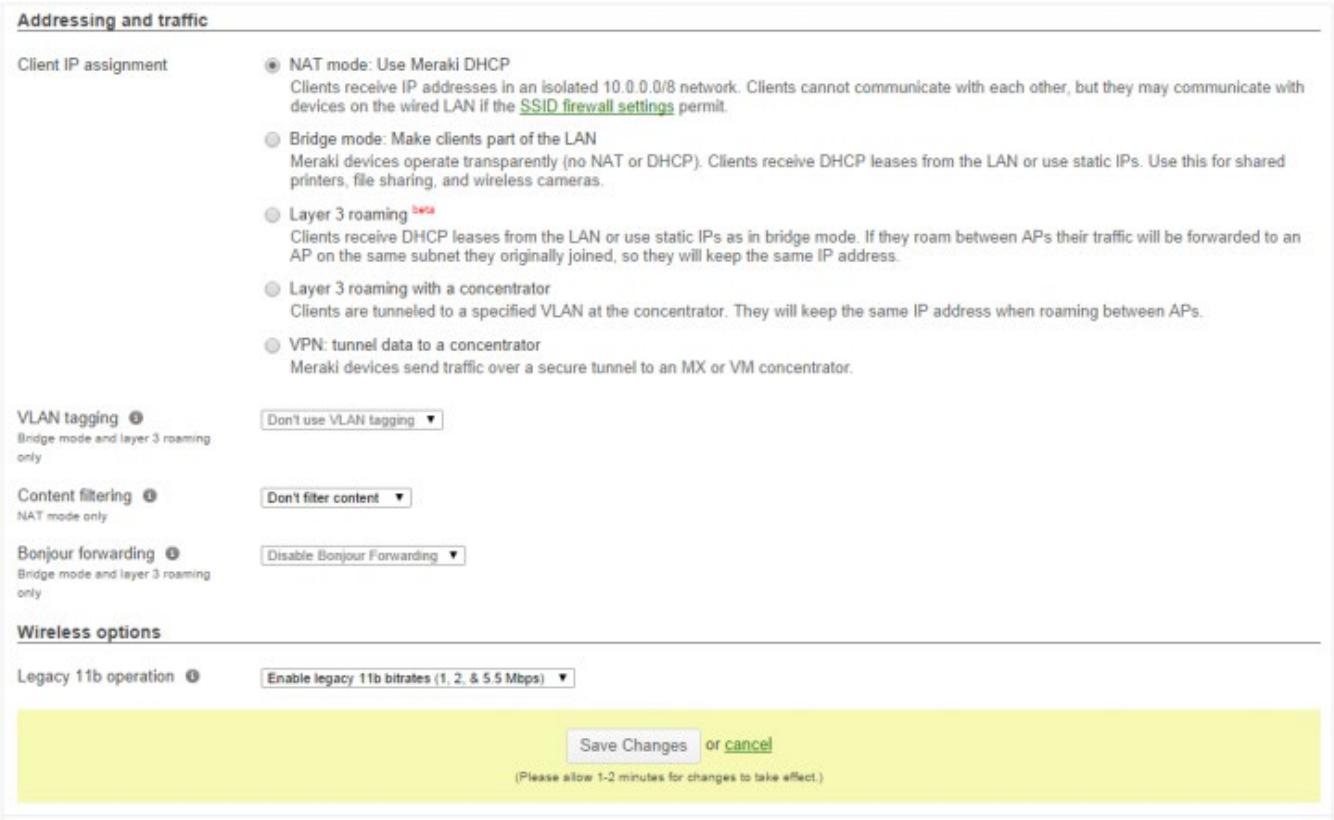


Рисунок 2.12 - Адресація і трафік

AP Meraki використовують VLAN на основі тегів для ідентифікації безпроводового трафіку на наступний по рівню комутатор чи маршрутизатор. Коли комутатор чи маршрутизатор бачить позначений VLAN трафік від точки

доступу Meraki, він може застосовувати до цього трафіку різні політики, включаючи управління доступом (наприклад, відправляти трафік прямо на міжмережевий екран для доступу тільки через Інтернет) або QoS (наприклад, встановлювати пріоритет трафіку на VOIP SSID). І навпаки, коли точка доступу отримує позначений VLAN трафік від наступного по рівню комутатора чи маршрутизатора, він перенаправляє цей трафік на правильний клієнт чи SSID. Точка доступу відкидає всі пакети з ідентифікаторами VLAN, які не пов'язані ні з одним з його безпроводових користувачів або SSID.

Маркування VLAN може бути налаштована для кожного SSID, користувача або типу пристрою [10, 12].

Тег VLAN для кожного користувача може застосовувати трьома різними способами:

– сервер RADIUS повертає атрибут Tunnel-Private-Group-ID в повідомленні Access-Accept, який вказує ідентифікатор VLAN, який повинен бути застосований до користувача безпроводової мережі. Цей ідентифікатор VLAN може перевизначати все, що може бути налаштоване в МСС (це може бути відсутність тегів VLAN або тега VLAN для кожного SSID). Щоб цей VLAN ID вступив в силу, для параметра «Перевизначення RADIUS» необхідно встановити значення «Відповідь RADIUS може перевизначити тег VLAN» на вкладці «Налаштування» на сторінці «Контроль доступу» в розділі «Налаштування VLAN»;

– сервер RADIUS повертає атрибут групової політики (наприклад, Filter-ID) у повідомленні Access-Accept. Атрибут групової політики вказує групову політику, яка повинна застосовуватися до користувача безпроводової мережі, перевизначаючи політику, налаштовану на самому SSID. Якщо групова політика включає ідентифікатор VLAN, ідентифікатор користувача VLAN групової політики буде застосований до користувача;

– на сторінці Відомості про клієнта клієнту можна вручну призначити групову політику. Якщо групова політика включає ідентифікатор VLAN, ідентифікатор користувача VLAN групової політики буде застосований до

користувача.

Групові політики можуть автоматично призначатися різним типам пристроїв, таким як Android, iPad, iPhone, iPod, Mac OS X, Windows тощо. Якщо групова політика включає ідентифікатор VLAN, тоді ідентифікатор VLAN групової політики буде застосовуватися до користувача і перевизначати будь-які налаштування VLAN для цього SSID або користувача.

Функція підтримки Bonjour може використовуватися, щоб дозволити Bonjour працювати в декількох VLAN. Якщо включити пересилання Bonjour, запити Bonjour від клієнтів з цього SSID будуть перенаправлятися в «VLAN служби», яку назначили. Також можна вибрати певні послуги, щоб включити пересилку Bonjour для обмеженого набору послуг, наприклад тільки для AirPlay.

Приклади мостового трафіку між двома клієнтами по SSID з різними VLAN і мостового трафіку між сервісами в проводяних і безпроводових мережах з різними VLAN, налаштованими для кожного [12, 18].

Щоб включити пересилку Bonjour, точка доступу повинна спочатку перебувати в режимі «Міст» або «Роумінг 3-го рівня». Після цього треба перейти в розділ «Налаштування»> «Контроль доступу»> «Bonjour forwarding».

Натиснувши Додати правило пересилання Bonjour, створюється нове правило пересилання (рис. 2.13).

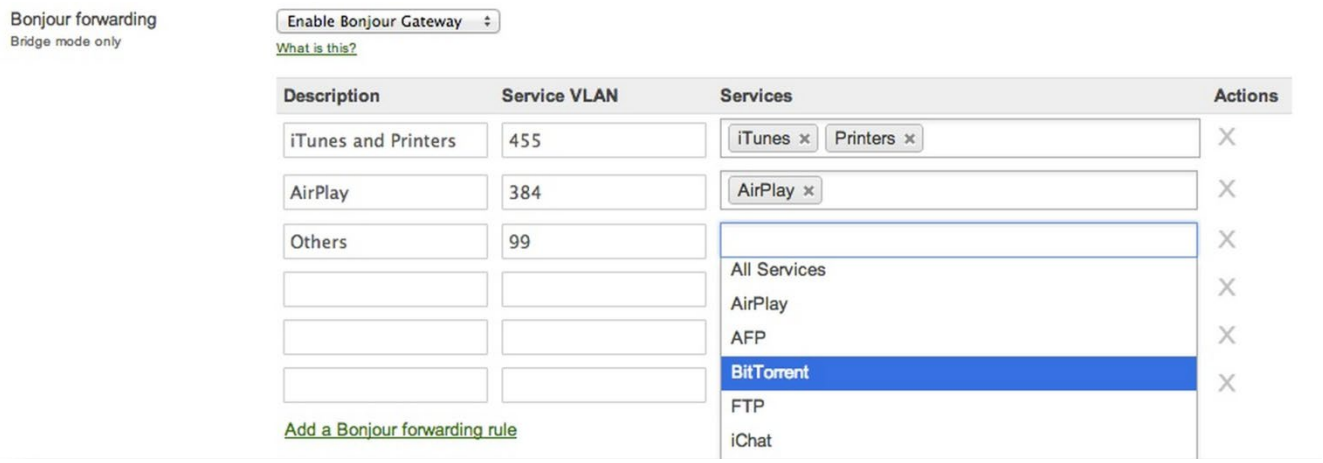


Рисунок 2.13 - Налаштування функції Bonjoir forwarding

Також в цьому пункті меню можна налаштувати параметри WiFi. В цьому

пункті вибираються частоти, на яких буде працювати точка доступу. Є можливість встановити, щоб 2,4 ГГц і 5 ГГц частоти працювали паралельно або тільки встановити активною 5 ГГц частоту. Також можна встановити щоб 2,4 ГГц і 5 ГГц частоти працювали паралельно, але з примусовим переключенням пристроїв, що підтримують 5 ГГц частоту.

Обравши роумінг третього рівня і частоти 2,4 та 5 ГГц з примусовим переключенням пристроїв, що підтримують 5 ГГц частоту переходимо до налаштувань Firewall і обмеження трафіку.

Meraki дозволяє обмежувати трафік на третьому і сьомому рівнях (рис. 2.14).

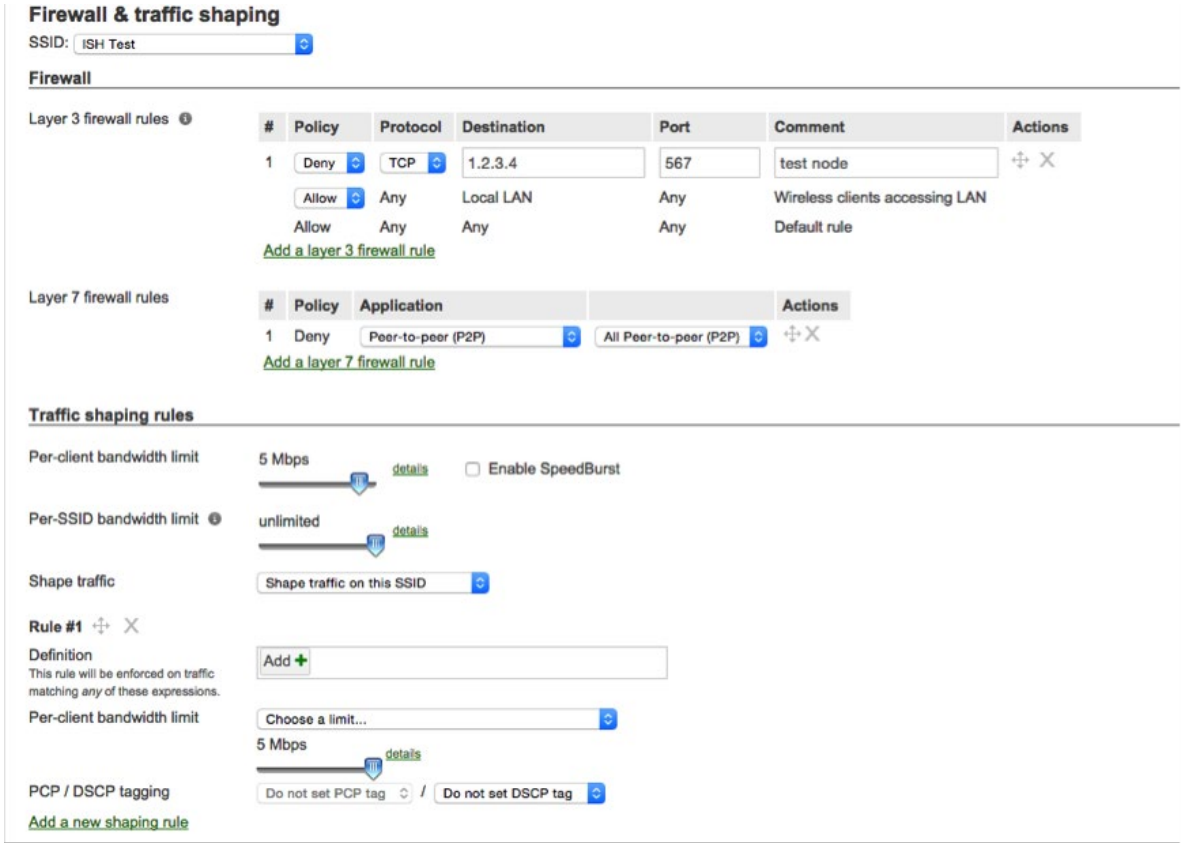


Рисунок 2.14 - Налаштування Firewall і обмеження трафіку

Призначені для користувача правила брандмауера надають більш детальний контроль доступу за межами ізоляції локальної мережі. Можна визначити набір правил брандмауера, який оцінюється для кожного запиту, відправленого безпроводовим користувачем, пов'язаним з певним SSID. Правила брандмауера

оцінюються зверху вниз. Перше відповідне правило застосовується, а наступні правила не оцінюються. Якщо не знайдено жодного правила, застосовується правило за замовчуванням (дозволити весь трафік).

Створили кілька правил для третього рівня (рис. 2.15). Різні типи запитів відповідають різним правилам. Згідно налаштувань для запиту BitTorrent правило 1 не збігається, але правило 2 збігається. Запит буде відхилений і ніякі подальші правила не оцінюються. Створили правило брандмауера «Deny Local LAN», щоб легко створити безпечний гостьовий SSID.

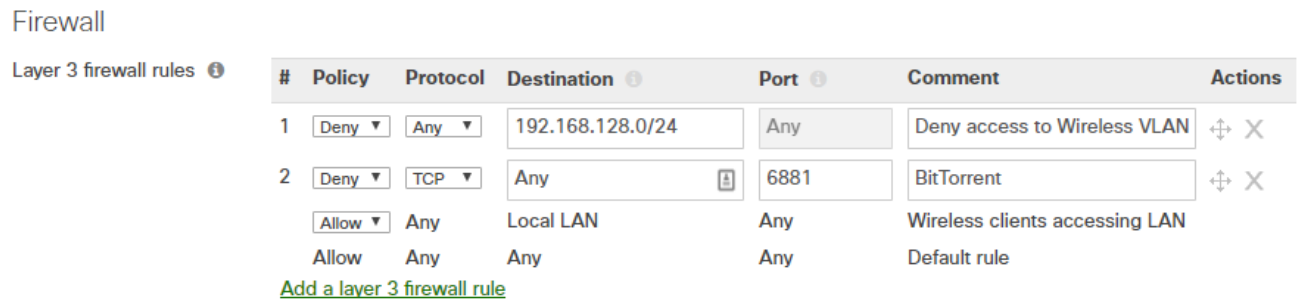


Рисунок 2.15 - Правила обмеження трафіку для третього рівня

Використовуючи унікальну технологію аналізу трафіку рівня 7 можна створювати правила брандмауера рівня 7, щоб повністю блокувати певні програми без необхідності вказувати конкретні IP-адреси або діапазони портів. Це може бути корисно, коли додатки використовують кілька або змінюють IP-адреси або діапазони портів. Можна блокувати програми по категоріям (наприклад, «Всі відео і музичні сайти») або для додатків певного типу в категорії (наприклад, тільки iTunes в категорії «Відео і музика»). На рисунку нижче показаний набір правил брандмауера рівня 7, включаючи додатки, заблоковані цілими категоріями, і конкретні програми, заблоковані всередині категорії.

Правила брандмауера можуть застосовуватися для даного SSID або як частина групової політики. Брандмауер рівня SSID налаштовується на сторінці "Wireless">"Firewall" і Traffic Shaping для кожного SSID.

Формування смуги пропускання гарантує, що користувачі не споживають велику смугу пропускання, ніж варто було б. Хмарне середовище Meraki включає

в себе вбудований модуль формування смуги пропускання, який забезпечує обмеження завантаження і вивантаження. Цей параметр можна використовувати, наприклад, для призначення більшої смуги пропускання для телефонів VOIP на одному SSID і меншою смуги пропускання для користувачів, що використовують тільки дані, на іншому SSID. Обмеження смуги пропускання застосовуються AP Meraki, тому вони застосовуються послідовно до безпроводового клієнта, навіть якщо цей клієнт переміщається від однієї AP до іншої.

Панель інструментів Meraki підтримує окремі обмеження на завантаження і скачування. Асиметричні обмеження завантаження і скачування корисні, наприклад, коли користувачеві потрібно тільки періодично завантажувати великі зображення (наприклад, креслення), але не завантажувати їх. Конкретні вимоги до додатка і доступна смуга пропускання повинні враховуватися для визначення оптимальних параметрів смуги пропускання.

Обмеження пропускної здатності можуть застосовуватися для кожного SSID або для кожного користувача. Щоб налаштувати обмеження смуги пропускання для кожного SSID, треба перейти на сторінку «Брандмауер і формування трафіку» на вкладці «Налаштування» [13, 14].

Щоб забезпечити кращу взаємодію з користувачем при використанні формування смуги пропускання, можна включити SpeedBurst за допомогою прапорця в розділі «Обмеження пропускної спроможності» на сторінці «Контроль доступу». SpeedBurst дозволяє кожному клієнту перевищувати свій призначений ліміт протягом короткого періоду часу, що робить його сприйняття більш швидким, в той же час не дозволяючи жодному користувачеві використовувати більш справедливу частку пропускної спроможності протягом більш тривалого терміну. Користувачеві дозволяється в чотири рази перевищувати межу виділеної смуги пропускання на термін до п'яти секунд.

Панель інструментів Meraki включає в себе параметри, що дозволяють підтримувати обмеження смуги пропускання для кожного користувача при використанні розміщеного на сервері RADIUS. Тобто кожній групі користувачів можна обмежити швидкість мережі по різному, задля збереження ресурсів

мережі.

Формування трафіку. За допомогою цього параметра можна створити політики формування, які будуть застосовуватися для користувача елементів управління для кожної програми. Це дозволяє регулювати рекреаційні програми, такі як однорангові програми обміну файлами, і визначати пріоритети корпоративних додатків, таких як Salesforce.com, гарантуючи, що критично важлива для бізнесу продуктивність додатків не береться до ризику.

Створили правила формування трафіку (рис. 2.23). Політики формування трафіку складаються з ряду правил, які оцінюються в порядку їх появи в політиці, аналогічно налаштованим правилами брандмауера. У кожного правила є два основних компоненти: визначення правил і дії правил.

Правила можуть бути визначені двома способами. Можна вибирати з різних існуючих категорій додатків, таких як відео і музика, однорангова зв'язок або електронна пошта. Другий метод визначення правил полягає у використанні для користувача визначень правил. Правила можна створити, вказавши імена хостів HTTP (наприклад, salesforce.com), номер порту (наприклад, 80), діапазони IP-адрес (наприклад, 192.168.0.0/16) або комбінації діапазонів і портів IP (наприклад, 192.168.0.0 / 16). : 80).

Трафік, що відповідає заданим набором правил, може бути сформований та мати пріоритет. Межі пропускної здатності можуть бути зазначені або вони будуть ігноруватися згідно налаштувань певного SSID.

Далі переходимо до налаштувань радіо сигналів. Присутня така функція як Auto Channel. Авто канал динамічно налаштовує канали клієнта, обслуговуючого радіостанції, щоб уникнути радіочастотних перешкод (як 802.11, так і не 802.11) і розробити план каналів для безпроводової мережі. Автоматичний канал добре підходить для більшості безпроводових мереж, надаючи базову конфігурацію каналу, яку потім можна налаштувати вручну, якщо це необхідно.

Автоматичний канал включений за замовчуванням на всіх точках доступу Meraki. Щоб переконатися, що автоматичний канал включений в точці доступу, потрібно обрати «Безпроводова мережа»> «Налаштувати»> «Налаштування

радіо» в «Особистому кабінеті» і вибрати конкретну точку доступу. Конфігурація радіо для точки доступу буде відображатися в правій частині сторінки. Алгоритм автоматичного каналу буде використовуватися на радіостанціях, для яких вибраний канал "Авто".

Вибір каналу 2,4 ГГц. При виборі Auto Channel панель моніторингу слід передовим практикам і галузевим стандартам, тому радіочастота 2,4 ГГц для точок доступу буде налаштована тільки на канали 1, 6 і 11. Оскільки вони не перекриваються по частоті, ці три канали мають найменшу кількість супутніх каналів. перешкоди в каналі. Інші канали включені в список і можуть бути обрані вручну для скасування алгоритму автоматичного каналу.

Вибір каналу 5 ГГц. Приватність каналу для 5 ГГц залежить від моделі точки доступу та області регулювання. Панель моніторингу буде розглядати будь-який канал, для якого точка доступу сертифікована, в області регулювання. Список каналів можна переглянути, відкривши список, що розкривається каналів для точки доступу на сторінці налаштувань радіо. Для конкретної смуги немає переваг, і всі канали зважені рівномірно.

Ширина радіоканалу. Панель інструментів пропонує можливість встановити ширину каналу за замовчуванням, яка буде врахована в алгоритмі автоматичного каналу для 5 ГГц. Параметр можна залишити на автоматичної ширині, яка буде регулювати ширину радіостанції 5 ГГц на основі алгоритмів автоматичного каналу, обговорюваних нижче. Значення за замовчуванням ширини 80 МГц може бути налаштоване для забезпечення оптимальної пропускної здатності безпроводового з'єднання, проте може привести до більшого конфлікту в суміщеному каналі. Параметр може бути зменшений до 40 або 20 МГц, щоб зменшити перекриття каналів при розгортанні з високою щільністю. Ширина каналу за замовчуванням може бути вказана на сторінці налаштувань радіо в Dashboard. Ширина може бути встановлена по-різному для кожної точки доступу або за допомогою перевизначень, клацнувши точку доступу, або вибравши Авто.

Точки доступу Cisco Meraki, які не підтримують канали шириною 80 МГц, за замовчуванням будуть мати ширину каналу 40 МГц.

3 РОБОТА З ХМАРНИМ СЕРВІСОМ УПРАВЛІННЯ CISCO MERAKI CLOUD MANAGER

3.1 Моніторинг комп’ютерної мережі Cisco Meraki

Сторінка стану точки доступу відображається зі списку точок доступу в розділі «Безпроводовий зв'язок»> «Точки доступу». Натисніть на будь-яку точку доступу, щоб переглянути сторінку стану точки доступу. Сторінка стану точки доступу містить наступну інформацію:

– ідентифікаційна інформація (серійний номер, модель, мітки і місце розташування);

– інформація про налаштованому IP-адресу (IP-адреса, метод призначення адреси, шлюз за замовчуванням і DNS-сервери, призначені для висхідній лінії зв'язку);

– загальнодоступна IP-адреса, яка в даний час використовується для зв'язку з Meraki Cloud;

– посилання на сторінку топології мережі (тільки для комбінованих мереж)

– посилання Журнал подій точки доступу;

– інформація про стан конфігурації, яка вказує, чи є актуальною конфігурація точки доступу;

– сконфігурована інформація про прошивку, яка вказує, що точку доступу оновлено на останню доступну виробничу прошивку, і посилання на сторінку, де оновлення може бути виконано або заплановано

Натиснувши "Змінити конфігурацію", можна редагувати ім'я, замітки, теги і інформацію про місцезнаходження для пристрою MR. Також можна видалити пристрій, натиснувши "Видалити з цієї мережі".

Активні інструменти на сторінці «Монітор»> «Точки доступу» можуть надати важливу інформацію і допомогти в усуненні неполадок. Щоб використовувати Live Tools, потрібно вибрати точку доступу на сторінці

«Монітор»> «Точки доступу». Є такі Live Tools:

- поточні клієнти;
- використання каналу;
- пінг;
- ARP таблиця;
- трасування;
- пропускна спроможність;
- поблимати світлодіодами;
- перезавантажити точки доступу;

Інструмент «Поточні клієнти» завантажується автоматично за замовчуванням і показує кількість підключених клієнтів, використання даних для точки доступу в цілому і для кожного користувача, а також, як добре і як довго користувач був пов'язаний (рис. 3.1). Також можна пропінгувати кожного підключеного в даний момент клієнта [14, 15].

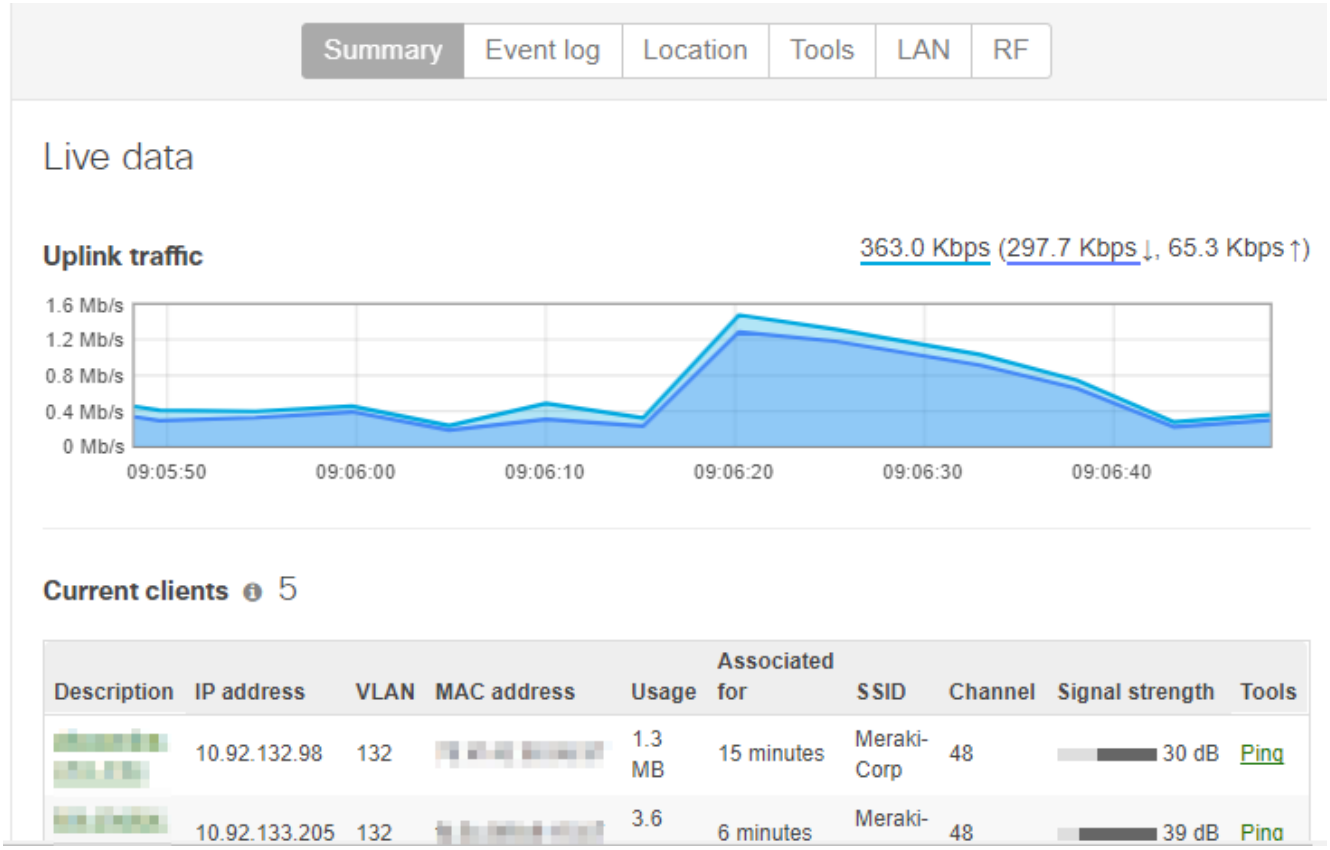


Рисунок 3.1 - Інструмент «Поточні клієнти»

Можна запустити тест Ping для будь-якого клієнта, який підключений до них по безпроводовому зв'язку (рис. 3.2). Це ARPing, і замість стандартного протоколу ICMP пристрій використовує протокол ARP. Це дозволяє звертатися до пристрою, навіть якщо є проблема з IP.

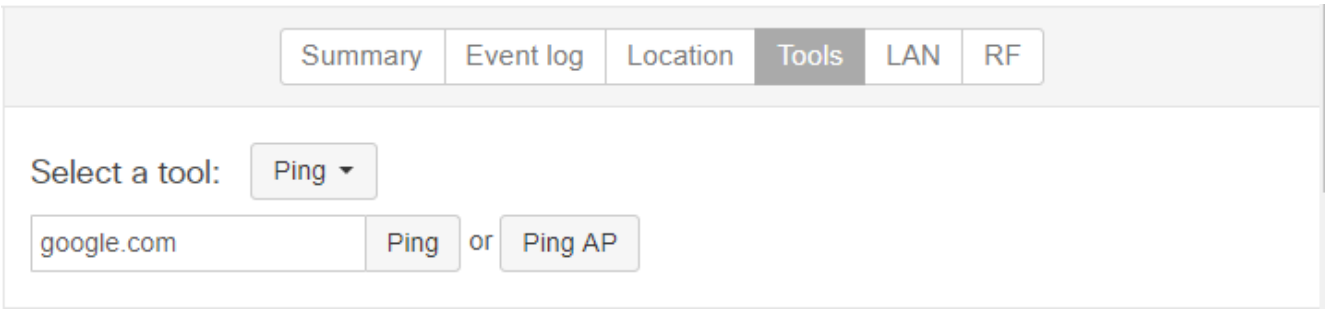


Рисунок 3.2 - Інструмент "Пінг"

За замовчуванням на хмарного контролера до точки доступу виконується ехо-запит, а потім можна запускати додаткові ехо-запити до клієнтів через MAC-адресу або ім'я клієнта.

Інструмент ARP Table Live використовується для перегляду таблиці ARP точки доступу. Це відобразить список IP-адрес і які MAC-адреси в даний час використовуються (рис. 3.3).

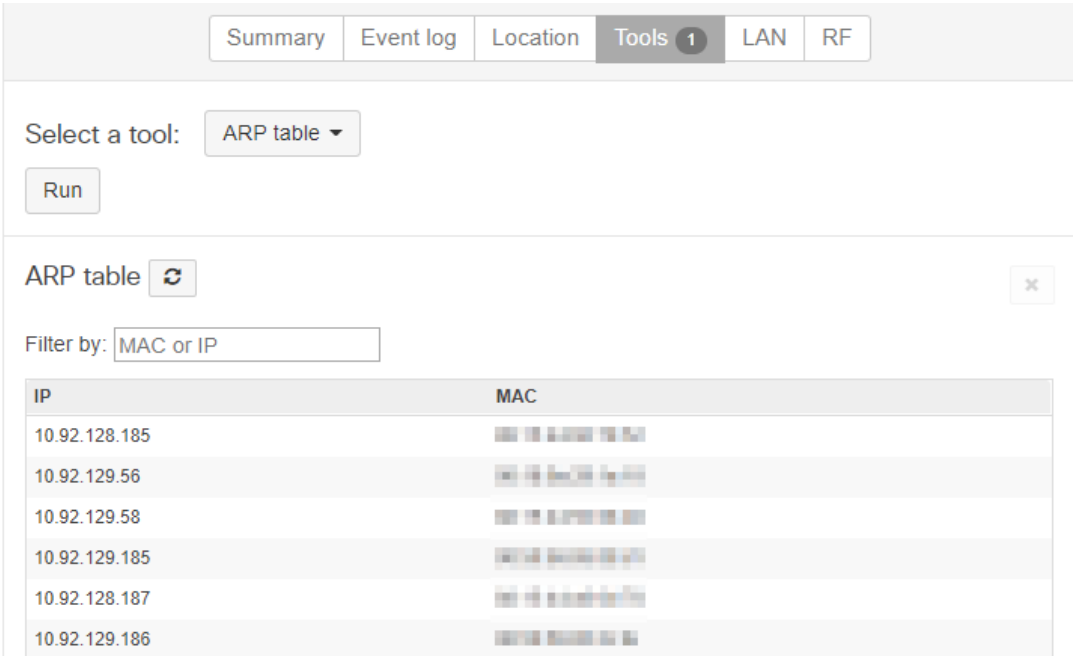


Рисунок 3.3 - Інструмент "ARP Table"

Можна запустити traceroute від AP до будь-якого хоста в висхідному напрямку. Це дозволяє дізнатися інформацію про маршрут від точки доступу до конкретного хосту (рис. 3.4).

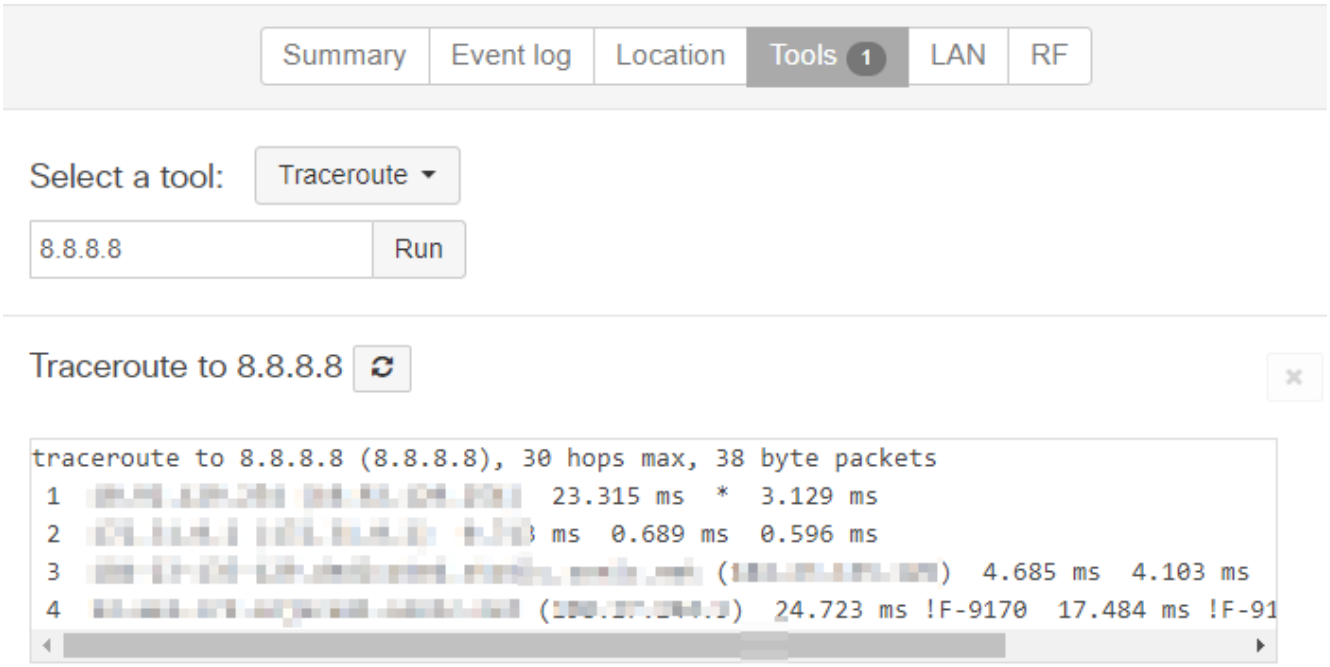


Рисунок 3.4 - Інструмент "Traceroute"

Інструмент "Throughput " дозволяє виконати тест пропускної здатності між точкою доступу і панеллю приладів, але це не є засобом перевірки загальної пропускної спроможності, доступної від точки доступу до Інтернету. Таким чином можна зрозуміти швидкість побудованої локальної мережі.

Інструмент "Blink LEDs" корисний для пошуку точки доступу. Крім того, якщо працювати в темному режимі, коли світлодіоди згасають, цей інструмент буде блимати світлодіодами, щоб можна було побачити, чи працює пристрій чи ні.

Перезавантаження точки доступу. Якщо точка доступу реєструється в хмарі, і потрібно виконати перезавантаження, щоб не відключати пристрій, можна запустити цю команду з панелі моніторингу.

Ці інструменти будуть працювати тільки з точками доступу, які знаходяться в мережі і взаємодіють з панеллю приладів. Якщо ви намагаєтеся

використовувати один з цих інструментів і їх завантаження займає багато часу, це може бути викликано декількома причинами:

Хмарне середовище Meraki дозволяє легко відстежувати стан багатьох точок доступу в мережі, а також трафік, що проходить по безпроводовій мережі. Більші розподілені клієнти, ймовірно, будуть мати кілька організацій.

Безпроводовий загальний звіт. Можна отримати розширену мережеву аналітику на сторінці «Загальний звіт» на вкладці «Монітор». Цей звіт містить інформацію про безпроводової мережі Meraki з моменту її створення, включаючи деякі з таких статистичних даних:

– топ 10 AP по споживанню даних і кількості входів клієнтів;
– топ 10 клієнтів по споживанню даних;
– розподіл використання по SSID і моделі AP;
– основні виробники клієнтських пристроїв і типи ОС за кількістю входів клієнтів і споживання даних.

Звіт можна налаштовувати і переглядати для статистики за певний період часу, щоб забезпечити статистичну аналітику за певний день, тиждень або місяць. Звіт можна надіслати електронною поштою за налаштованим розкладом для постійної видимості. Можна налаштувати одину або декілька адрес електронної пошти на вкладці «Розклад щомісячних електронних листів», якщо потрібно відправити загальний звіт декільком людям.

Поруч з графіком використання у верхній частині екрану знаходиться кругова діаграма, яка може відображати розбивку трафіку, відображуваного в даний момент на сторінці, за додатками, типу вмісту HTTP, номеру порту або призначеним для користувача критеріям (рис. 3.5). Сірі стрілки перевертаються з одного графіка на інший. Настроювати кругові діаграми можна на сторінці «Мережеві налаштування» на вкладці «Налаштування».

Якщо клацнути або саму кругову діаграму, або посилання «Ще» під круговою діаграмою, відкриється сторінка «Подробиці аналізу трафіку», в якій показано докладний список конкретних програм і типів контенту, що становлять дані, які відображаються на круговій діаграмі. Додатки були розподілені по

групах для спрощення класифікації додатків та формування політик формування.

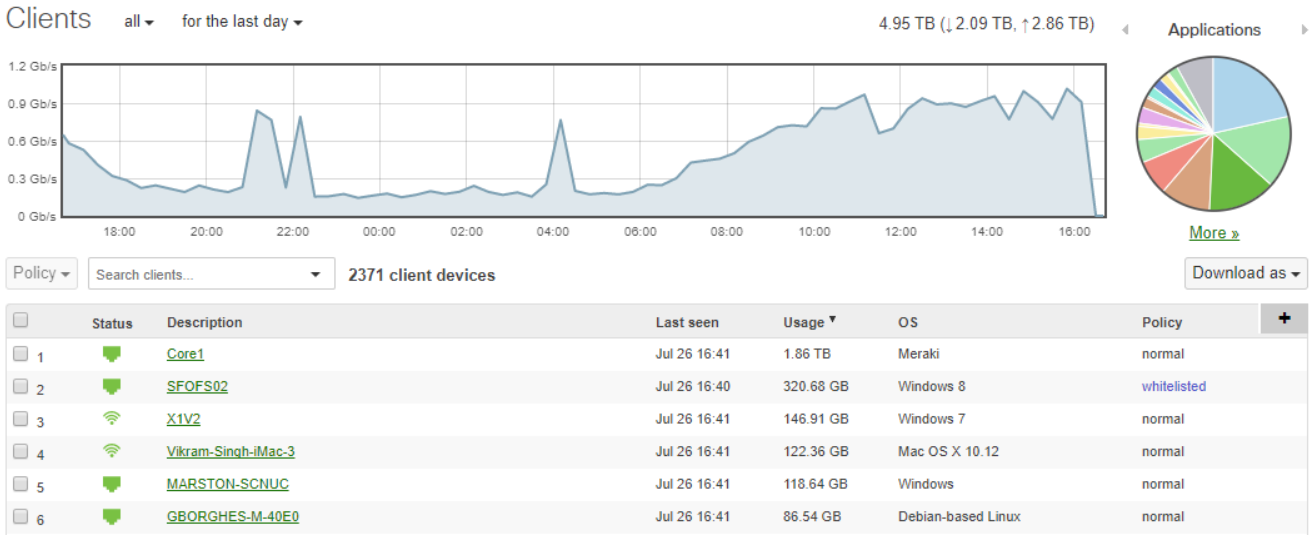


Рисунок 3.5 - Аналітика трафіку

На сторінці «Клієнти» показано, як використовується мережу і якими клієнтськими пристроями. Сторінка включає в себе наступні функції [15]:

– показує клієнтів, які були пов'язані з будь-яким SSID, оголошеним безпроводовою мережею, або тільки тих клієнтів, які були пов'язані з конкретним SSID;

– пошук клієнтів по MAC, ОС або по типу пристрою;

– елемент управління масштабуванням, який дозволяє бачити тільки тих клієнтів, які були пов'язані за вказаний проміжок часу;

– можна переглянути тільки тих клієнтів, які знаходяться в чорному списку MAC;

– у стовпці «Опис» відображається ім'я пристрою, якщо воно може бути визначено, в іншому випадку він просто відображає MAC-адресу пристрою;

– стовпець «Операційна система» показує операційну систему пристрою, яка визначається за допомогою зняття відбитків ОС (унікальний шаблон, за яким конкретна операційна система запитує IP-адреса через DHCP);

– можна переглянути частку загальної смуги пропускання, використовуваної виділеним пристроєм.

Список точок доступу - це зручний спосіб полегшити пошук, сортування і фільтрацію точок доступу у великій мережі з сотнями або тисячами точок доступу, що використовують мітки точок доступу.

Повітряна карта показує останню інформацію про точки доступу в мережі. Параметри у верхньому правому куті дозволяють переглядати точки доступу поверх графічної карти, супутникового зображення або гібридного зображення. У верхньому лівому кутку елементи управління стрілкою дозволяють панорамувати. Панорамування також може бути досягнуто шляхом натискання і перетягування карти. Нижче елементів управління стрілкою елемент управління масштабом дозволяє регулювати рівень масштабування. Рівень масштабування також можна контролювати за допомогою збільшувального скла поруч зі стрілками або подвійним клацанням миші по певній галузі для збільшення.

Можна натиснути на точку доступу, щоб дізнатися її ім'я, режим сітки (шлюз сітки або ретранслятор сітки), кількість користувачів, які зв'язалися з нею за останні 24 години (також позначається номером всередині точки доступу), і обсяг даних, які вона передала за останні 24 години. Сірі лінії між точками доступу є сітчасті посилання. При наведенні покажчика миші на повторювач осередків виділяється лінія, що показує шлях, по якому точка доступу проходить через порожнисту мережу, щоб досягти пористого шлюзу (і локальної мережі).

Якщо клацнути посилання «Поточні клієнти» під ім'ям мережі у верхньому лівому кутку, відкриється таблиця, в якій представлена зведена інформація про розподіл поточних клієнтів на даний момент з різних ідентифікаторів SSID і каналах в мережі.

Якщо клацнути посилання прямо над ім'ям мережі у верхньому лівому кутку або вибрати параметр «Огляд всієї мережі» в списку «Мережа» в верхній частині екрану, відбудеться перехід на сторінку «Огляд всієї мережі».

Системний журнал подій. Точки доступу Meraki можна налаштувати для відправки даних системного журналу на будь-який сервер, який приймає трафік системного журналу, на сторінці "Загальномережеві">"Загальні налаштування" (рис. 3.6). В даний час підтримується наступна інформація:

– журнали подій;
– журнали URL;
– транспортні потоки.

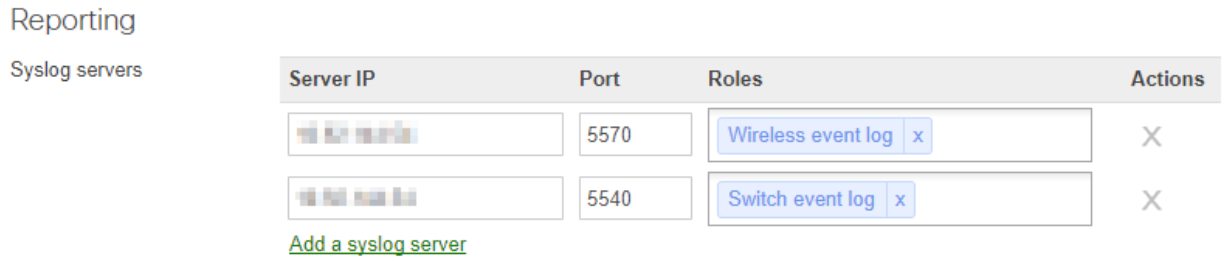


Рисунок 3.6 - Передача журналу подій на сервер

3.2 Аналітика на місцях комп'ютерної мережі Cisco Meraki

Завдяки стрімкому поширенню мобільних пристроїв, багато організацій тепер мають змогу використовувати дані для глибшого аналізу моделей та поведінки трафіку у своєму повсякденному середовищі. Ці дані про місцезнаходження, які в основному отримані через стандарти бездротового зв'язку і Bluetooth 802.11, можуть бути застосовані для покращення залученості користувачів та оптимізації маркетингових стратегій. У роздрібній торгівлі це може допомогти в боротьбі з такими тенденціями, як ерозія продажів в магазинах онлайн-магазинами, які протягом багатьох років мали доступ до аналогічних даних за допомогою аналітики, виробленої онлайн-інструментами (наприклад, коефіцієнтами переходів за кліками в онлайн-рекламі).

Смартфони з WiFi тепер можуть слугувати як індикатори присутності клієнтів завдяки загальнопоширеній функції в усіх таких пристроях: відправці перевірочних запитів. Ці керуючі рамки 802.11 передаються через регулярні проміжки часу від WiFi-пристроїв. Вони містять дані, які можна використовувати для визначення наявності клієнтів, вимірювання часу перебування та фіксації повторних візитів у районі дії WiFi. Ці пристрої виявляються точками доступу

WiFi, незалежно від того, чи підключено пристрій до мережі, що дозволяє визначити присутність користувача, якщо тільки його пристрій знаходиться в зоні дії мережі та WiFi антена пристрою активована.

Оскільки смартфони зараз э у половини населення, пробні запити можна використовувати для створення і виявлення статистично значимого набору даних, що стосуються присутності пристроїв з підтримкою WiFi в зоні дії даної точки доступу. Точки доступу Meraki та хмарна інфраструктура збирають ці дані і відображають їх агреговано на панелі інструментів Meraki за допомогою інтуїтивно зрозумілих та налаштованих графіків. Ці графіки допомагають аналізувати різні тренди, такі як коефіцієнт захоплення (кількість перехожих та відвідувачів), залученість користувачів (загальний час перебування) та лояльність відвідувачів (частота нових і повторних візитів). Використання передових хмарних технологій дозволяє Meraki надавати цю аналітику всім організаціям. Крім того, Meraki Scanning API дозволяє експортувати необроблені дані з протоколів спостереження для прямої інтеграції зі сторонніми системами зберігання даних або аналітики. Це відкриває можливості для глибшої інтеграції з традиційними системами управління відносинами з клієнтами (CRM) та сприяє залученню нового покоління клієнтів завдяки можливостям обробки даних в реальному часі.

В цілому, вбудовані уявлення Meraki для аналізу місця розташування та API визначення місцеположення в реальному часі доповнюють існуючі функції аналізу трафіку і дають повне уявлення про пристрої в межах і в межах діапазону мережі Cisco Meraki. Розглянемо це більш детально. Збір даних про місцезнаходження. Точки доступу Cisco Meraki генерують підпис присутності з будь-якого пристрою з підтримкою WiFi, виявляючи пробні запити і фрейми даних 802.11, незалежно від того, пов'язано пристрій з мережею чи ні. Пристрої WiFi зазвичай відправляють пробний запит через регулярні проміжки часу в залежності від стану пристрою (рис. 3.7). Смартфони відправляють тестові запити для виявлення оточуючих безпроводових мереж, щоб вони могли зробити мережі доступними для користувача.

Device State	Probe Request Interval (smartphones)
Asleep (screen off)	~ once a minute
Standby (screen on)	10 - 15 times per minute
Associated	varies, could require user to manually search for networks

Рисунок 3.7 - Інтервал запиту, що спостерігається у смартфонів

Фрейми даних, отримані від всіх підключених WiFi-пристроїв, і тестові запити, виявлені з усіх пристроїв, видимих в радіусі дії, генерують події «побаченого пристрою» в точках доступу Meraki. Точки з потрійним радіомодулем приймають тестові запити постійно на всіх каналах. Точки доступу з двома радіостанціями, в яких відсутня сканируюча радіостанція, можуть чути запити на сканування, коли пристрої WiFi проводять сканування по всіх каналах. Отримана інформація про пристрій завантажується через захищений тунель управління між точкою доступу і хмарним середовищем Meraki.

Тунель безпечного управління Meraki високо оптимізований для надсилання та отримання статистики конфігурації і великих обсягів інформації, а додаткові витрати від перегляду даних пристрою практично незначні; загальна смуга пропускання, яка використовується тунелем управління, залишається близько 1 кбіт/с.

Точки доступу Meraki також визначають рівень сигналу фреймів даних і перевірочних запитів, які можна використовувати для оцінки фізичного положення пристроїв WiFi.

Агрегування і відображення даних. Після отримання хмарним середовищем Meraki сигнатури присутності від усіх точок доступу в мережі дані агрегуються. Після агрегування, дані від кожного спостережуваного клієнтського пристрою піддаються серії обчислень, щоб класифікувати їх для подальшого подання (рис. 3.8). Наприклад, роздрібні продавці повинні розуміти швидкість захоплення, яка представляє собою співвідношення кількості людей, що проходять повз магазин, і фактичної кількості відвідувачів. Щоб визначити частоту захоплення, хмарне середовище Meraki аналізує рівень сигналу кожного клієнтського пристрою, а також час, проведений в цьому місці.

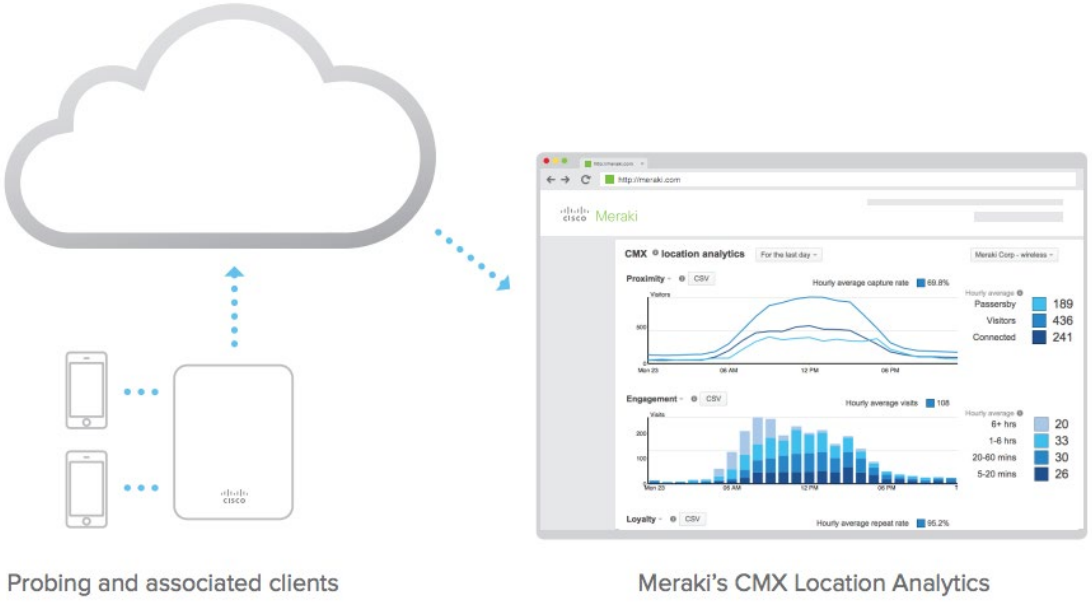


Рисунок 3.8 - Приклад процесу агрегування і відображення даних

У той час як хмарне середовище Meraki виконує вищенаведені обчислення в режимі реального часу для розрахунку різних станів клієнтів, панель інструментів Meraki відображає її за допомогою інтуїтивно зрозумілих графіків, які візуалізують рівень захоплення, залученість і лояльність. Ці графіки можна перемикати між простими і складними уявленнями. Функція календаря дозволяє користувачеві збільшувати або зменшувати заданий проміжок часу, щоб переглядати деталізовані перегляди за один день (який може показати, як змінюється інтенсивність руху і максимуми протягом певного дня) або до декількох місяців (який може відображати сезонні коливання) [16].

Доступна функція календаря часу, що дозволяє вибирати певні періоди часу для перегляду. Це дозволяє відрегулювати вісь X вищенаведених графіків для перегляду даних за певний період часу, наприклад, як кількість відвідувачів змінилося протягом певного дня або тижня (рис. 3.9). Дані аналізу місця розташування мають 1 рік зберігання для щоденної аналітики, 3 місяці для щогодинної аналітики.

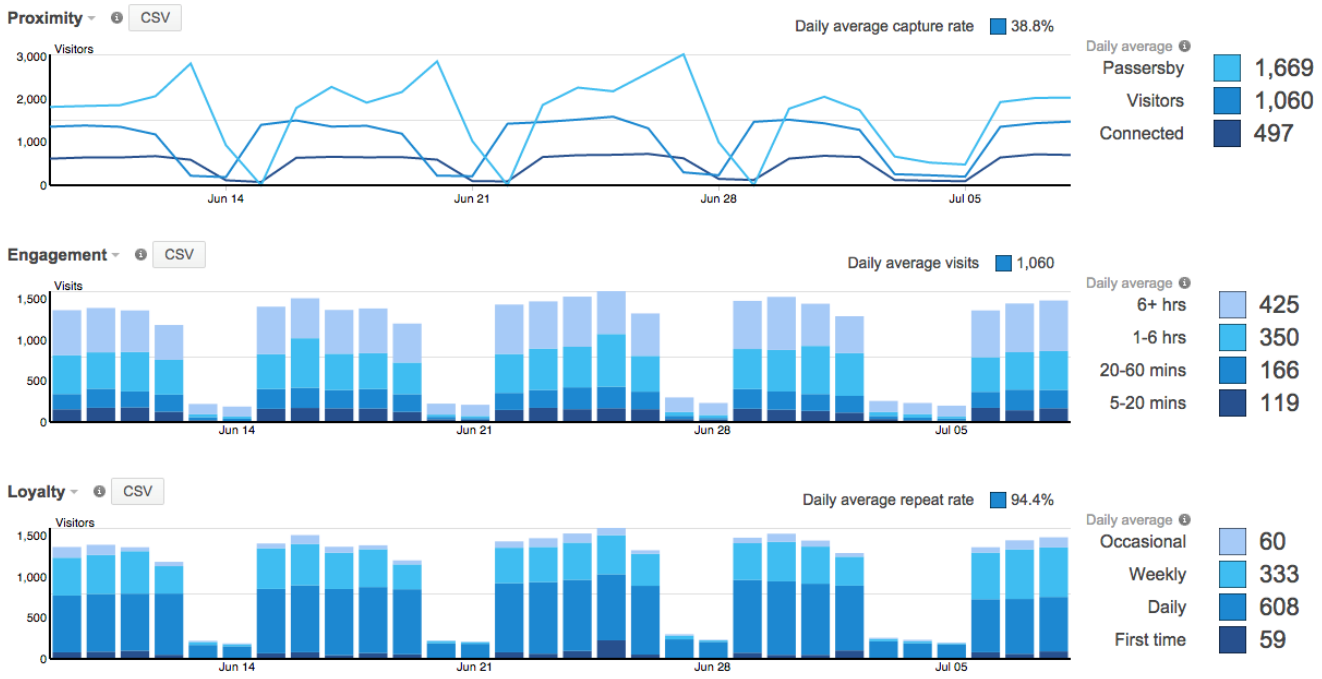


Рисунок 3.9 - Приклад графіку рівеня захоплення, залученості і лояльністі клієнтів

«Коефіцієнт захоплення» - це відсоток перехожих, які стають відвідувачами. «Відвідувачі» - це безпроводові пристрої, які «відвідували» вашу мережу. Відвідування починається, коли AP Meraki виявляє зонд з силою сигналу 15 dBm або більше. «Відвідувачі», підраховані на графіку близькості, враховуються тільки один раз для відповідної сесії. Якщо відвідувач не залишав зону покриття певний період, то відвідувачем він стає, як тільки потрапляє під зону дії точки доступу. Період, який він провів в зоні дії точки доступу уже є данними графіку залученості. «Відвідувач» - це безпроводові пристрої, які підтримують високий рівень сигналу протягом більше 5 хвилин. Це дозволяє визначити, скільки відвідувачів заходять в певний час і скільки часу вони залишаться. Останній графік показує відвідувачів в залежності від того, як часто вони повертаються. Наприклад, щотижневий відвідувач - це той, хто повертався від 2 до 6 разів за останній місяць.

Сканування API доставляє дані в режимі реального часу з хмари Meraki і може використовуватися для виявлення пристроїв WiFi і Bluetooth Low Energy (BLE) в режимі реального часу. Елементи експортуються через HTTP POST даних

JSON на вказаний цільової сервер (рис. 3.10). Необроблені дані агрегуються з усіх точок доступу в мережі в хмарному середовищі Meraki і відправляються безпосередньо з хмарного середовища в сховище даних організації або центр бізнес-аналітики. Повідомлення JSON відбуваються часто, як правило, пакетуються кожну хвилину для кожної точки доступу.

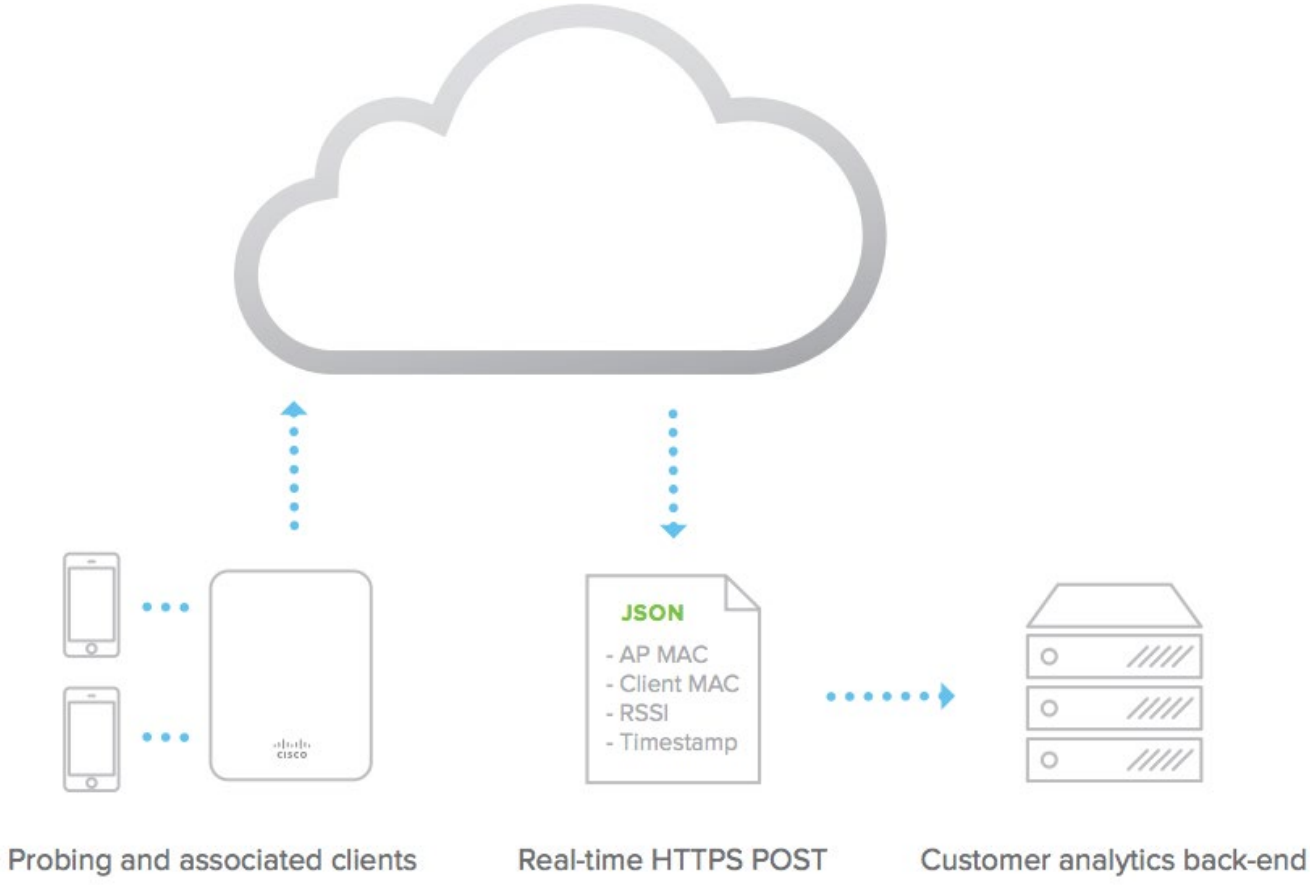


Рисунок 3.10 - Схема сканування API

Використовуючи фізичне розміщення точок доступу з Map&Floorplan на Dashboard, хмарне середовище Meraki оцінює місце розташування клієнта. Координати географічного розташування (широта, довгота) і точність даних розташування координат X, Y можуть варіюватися в залежності від ряду факторів. Розташування точки доступу, умови навколишнього середовища і орієнтація клієнтського пристрою можуть впливати на оцінку координат X, Y. Коригування розміщення точок доступу або додавання додаткових точок доступу

може допомогти підвищити точність результатів. Зазвичай для фільтрації точок даних вибирають мінімальне значення сили сигналу, максимальне значення невизначеності або інші елементи даних, включені в API.

API-інтерфейс сканування налаштовується в Meraki Dashboard на сторінці "Network Wide"> "General settings" в кілька простих кроків:

– потрібно налаштувати і розмістити HTTP-сервер для отримання об'єктів JSON;

– потрібно увімкнути API, вибравши Scanning API enabled в списку;

– потрібно вказати URL-адресу публікації і секрет аутентифікації;

– треба вибрати, яку версію API сканування HTTP-сервер готовий прийняти і обробити;

– треба натиснути кнопку «Підтвердити» і, при успішній перевірці, натиснути кнопку «Зберегти», щоб зберегти сторінку.

API сканування Cisco Meraki експортує необроблені MAC-адреси на вказаний сторонній сервер. Cisco Meraki впровадили ряд механізмів захисту конфіденційності, в тому числі:

– немає механізмів прив'язки особистості клієнта. Cisco Meraki не надає прямого зв'язку між MAC-адресами і ідентифікацією клієнта. Ці системи повинні бути побудовані окремо і розміщуватися клієнтом, партнером чи постачальником послуг.

– немає механізмів зв'язку з клієнтами. Cisco Meraki не надає будь-якого механізму, за допомогою якого дані API можуть використовуватися для зв'язку з клієнтами будь-яким способом. Для взаємодії з користувачами в режимі реального часу клієнти Cisco Meraki повинні створити і підтримувати власну платформу для зв'язку з клієнтами.

Meraki випустила мобільні додатки для iOS і Android, можливості у них досить мізерні, але відстежувати трафік за допомогою них можна (рис. 3.11) [17].

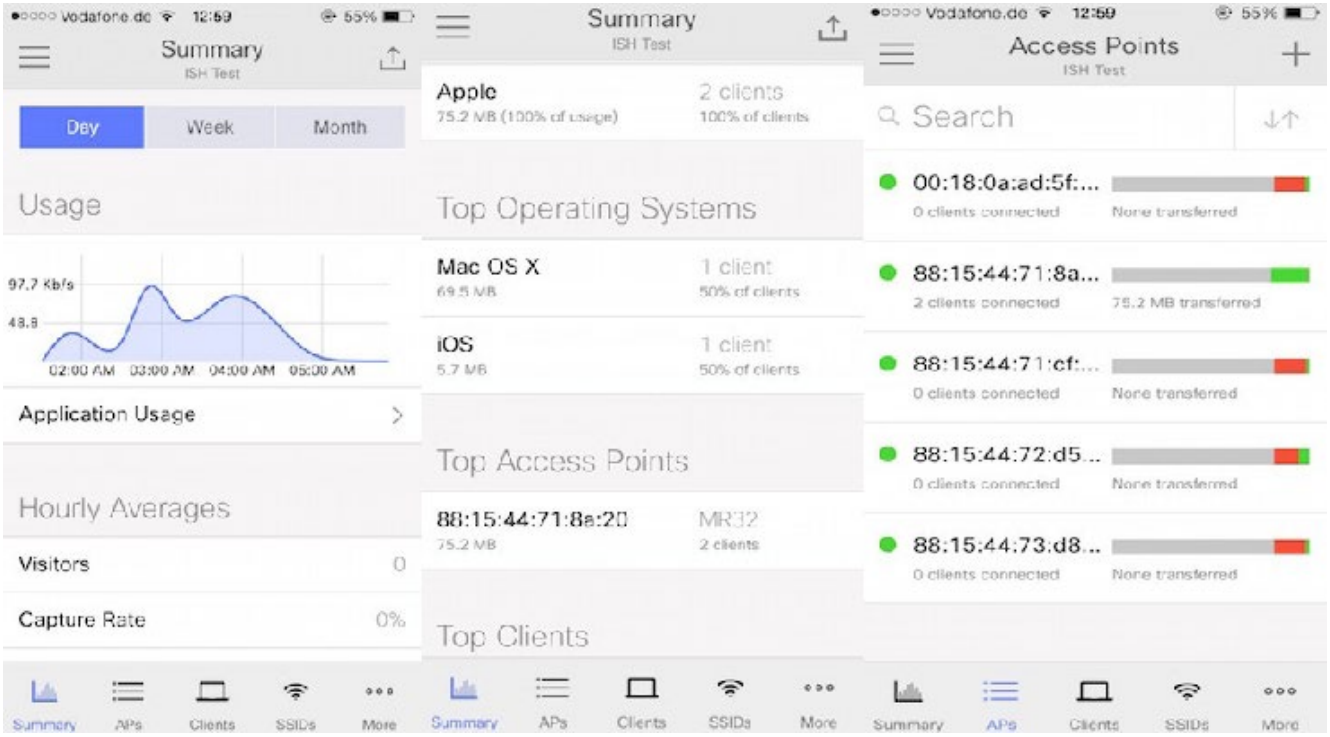


Рисунок 3.11 - Приклад використання мобільного додатку Cisco Meraki

ВИСНОВКИ

В бакалаврській роботі проаналізовано пристрої Cisco Meraki, як основний принцип побудови локальної мережі, для організації ефективного функціонування та спрощеного адміністрування мережі.

Практична частина роботи полягає у налаштуванні програмного забезпечення точок доступу Cisco Meraki та дослідженні хмарного сервісу управління Cisco Meraki Cloud Manager. Було впровадженно архітектуру Cisco Meraki в мережу і налаштованні обладнання даної архітектури в цій мережі. Визначено загальні переваги та недоліки данної архітектури.

Зроблено висновок, що дана архітектура є гарним вибором в розширенні або побудові комп'ютерної мережі в цілому. Досліджено та запропоновано до реалізації архітектуру Cisco Meraki, як лінійку провідних рішень на ринку для організації безпечних і високонавантажених Wi-Fi-мереж. Визначено, що побудовані за допомогою Cisco Meraki безпроводові мережі прості в розгортці, легкі в управлінні, надійні, піддаються масштабуванню і працюють безвідмовно.

Сфера застосування, де подібні пристрої могли б стати в нагоді, досить широка. Це і університетські кампуси, і ресторани, і готелі, бібліотеки, концертні зали.

ПЕРЕЛІК ПОСИЛАНЬ

1. Importance of information technology in today world *URL:* https://medium.com/@niyajohn9495/importance-of-information-technology-in-today-world-dba3d6bd2eb2

2. Information Technology & Its Role in the Modern Organization *URL:* https://smallbusiness.chron.com/information-technology-its-role-modern-organization-1800.html

3. Cisco Meraki Wireless Access Points *URL:* https://meraki.cisco.com/products/wireless (дата звернення 13.04.2020)

4. Meraki Cloud Architecture *URL:* https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Meraki_Cloud_Architecture

5. Б. Платтнер, В. Чернега. Безпровідні локальні комп’ютерні мережі - Київ: Кондор, 2018. - 238 с.

6. Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. - Львів: «Магнолія 2006», 2015. - 256 с.

7. Александр Латкин. Технологии, которые изменили мир - М.: «Манн, Иванов и Фербер», 2013. - 360 с.

8. Буров Є. В. Комп'ютерні мережі: підручник / Є. Буров. - Львів: «Магнолія 2006», 2014. - 262 с.

9. J. Florwick, J. Henry. "Designing and Deploying 802.11n Wireless Networks". Cisco Press, 2010.

10. V. Moreno, R. Zamora. "Enterprise Mobility Suite Managing BYOD and Company-Owned Devices". Cisco Press, 2015.

11. R. A. Mazzucchelli, T. Miller. "Implementing Cisco Unified Wireless Networking Essentials (IUWNE): Foundation Learning Guide". Cisco Press, 2012.

12. D. D. Hucaby, D. L. Hutton, B. T. Rasika. "Implementing Cisco Wireless Network Fundamentals (WIFUND): Foundation Learning Guide". Cisco Press, 2016.

13. S. Tomé, T. Carpenter. "Mastering Wireless Penetration Testing for Highly-

Secured Environments". Packt Publishing, 2015

14. Каталог обладнання Cisco Meraki *URL:* https://rci-c.com/items-catalog/tochky-dostupu/page/2/.

15. Introduction to Cloud Managed Networking. *URL:* https://www.cisco.com/c/dam/global/hr_hr/assets/ciscoconnect/2013/pdfs/cisco_presentation_meraki_paul_franka.pdf.

16. Курс CCNA IntroductionToNetwork. *URL:* www.netacad. com.

17. Документація про технології та продукцію Cisco Meraki (meraki.cisco.com) *URL:* https://documentation.meraki.com/MR.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ