НАПРЯМ 10. МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

Скопень Микола Максимович
кандидат економічних наук, доцент,
викладач-методист кафедри загальнотеоретичної
та прикладної підготовки;

Будя Олександр Петрович
кандидат технічних наук, доцент,
викладач-методист кафедри загальнотеоретичної
та прикладної підготовки;

Стародуб Олександр Петрович
викладач-методист, голова циклової комісії
«Програмування та спеціальних інформаційних дисциплін»,
Київський фаховий коледж туризму
та готельного господарства

DOI: https://doi.org/10.36059/978-966-397-296-1-29

ОСОБЛИВОСТІ ПОБУДОВИ ТА ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ З ВИКОРИСТАННЯМ ПРИСТРОЇВ MERAKI

Пристрої *Meraki* (www.meraki.cisco.com) розробляються IT-компанією *Cisco-Meraki* (м. Сан-Франциско, штат Каліфорнія) для посилення безпеки бездротових мереж, поліпшення їх структуризації та забезпечення можливості віддаленого адміністрування за допомогою хмарних технологій. До основних таких пристроїв можна віднести, наприклад, пристрій безпеки *Meraki-MX65W Security Appliance* та *Meraki*-сервер, яким дана достатня загальна характеристика [2]. Однак, до цього треба додати, що *Meraki-MX65W* оснащений модулем *WiFi 802.11ac* та має 12 портів, два з яких підтримують технологію *Power over*

Ethernet (PoE), тобто можливість передавати електричне живлення по крученій парі.

Слід зауважити, що деякі літературні джерела розкривають або основи створення та налаштування бездротової мережі [1, с. 186], або технології посилення безпеки бездротових мереж шляхом підключення пристроїв Meraki до дротових мереж [3], або захист бездротової мережі (*Wireless Local Area Network, WLAN*) шляхом безпосереднього шифрування даних на її вузлах та обмеження доступу на маршрутизаторі [4]. Однак, аналіз видань свідчить про відсутність розкриття технології побудови та дистанційної організації захисту, наприклад, двох і більше *WLAN* на платформі пристроїв *Meraki*. Саме ця технологія і пропонується авторами нижче для розгляду.

Припустимо, що в корпоративній мережі треба побудувати та організувати віддалено захист двох *WLAN*. В даному випадку порядок дій буде складатися з наступних етапів:

− побудова топології двох *WLAN* на базі *Meraki-MX65W* з віддаленим адмініструванням за допомогою *Meraki* – сервера (рис. 1);

− налаштування роутера для забезпечення зв’язку пристрою безпеки *Meraki-MX65W* з *Meraki* – сервер;

− налаштування параметрів пристрою безпеки *Meraki-MX65W*;

− налаштування через хмарний сервер *Meraki* бездротового зв’язку користувачів та шифрування даних.

Побудова топології двох WLAN передбачає:

− встановлення *Meraki* – сервера та налаштування його IP-конфігурації: *IPv4 Address* – 10.1.1.2, *Subnet Mask* – 255.0.0.0 та *Default Gateway* – 10.1.1.1;

− встановлення роутера з трьома мережевими картами *PT-ROUTER-NM-1CGE (Cisco Gigabit Ethernet Network Module)* і налаштування його IP-конфігурації: шлюз *GigabitEthernet0/0 – IPv4 Address* – 10.1.1.1, *Subnet Mask* – 255.0.0.0; шлюз *GigabitEthernet1/0 – IPv4 Address* – 9.1.1.1, *Subnet Mask* – 255.0.0.0; шлюз *GigabitEthernet2/0 - IPv4 Address* – 11.1.1.1, *Subnet Mask* – 255.0.0.0;

− з’єднання роутера кросовером з *Meraki* – сервером (порт Gig0/0) та двома пристроями безпеки (підключення до порту *Internet1*).

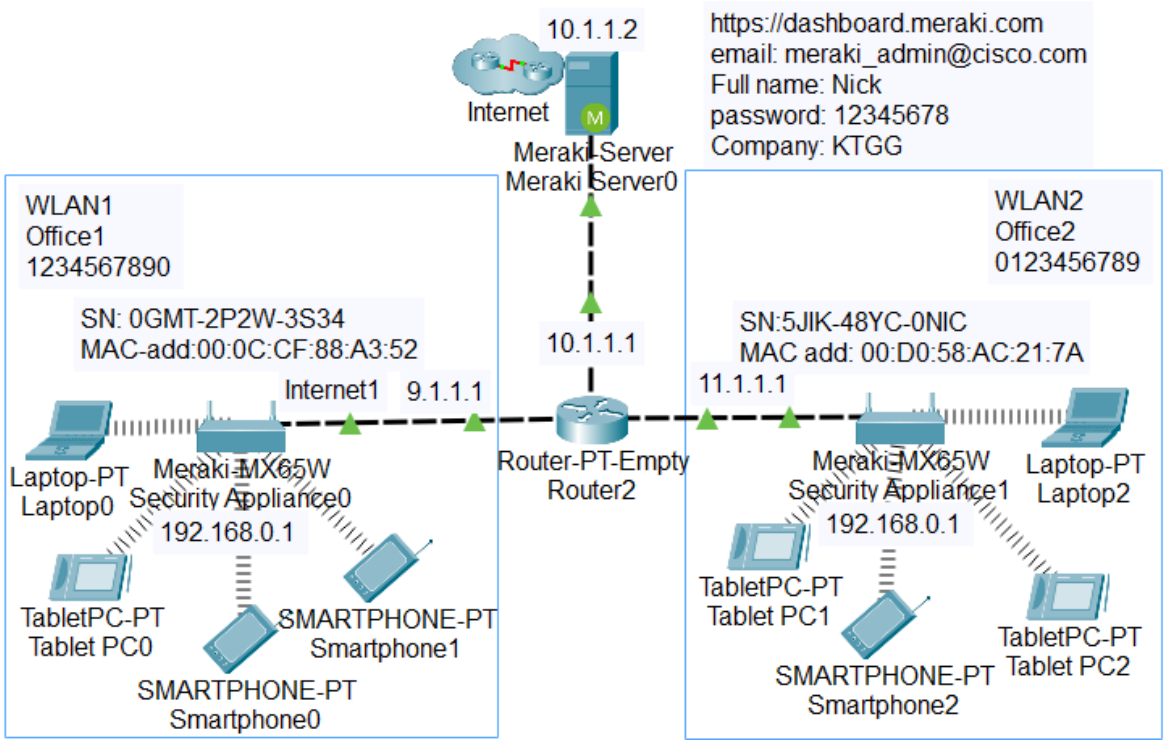

Рис. 1. Топологія двох WLAN на базі Meraki-MX65W з віддаленим адмініструванням за допомогою Meraki – сервера

Налаштування роутера – це запуск служби *DHCP (Dynamic Host Configuration Protocol)* для встановлення IP-адреси портам *Internet1* пристроям безпеки, відповідно, *WLAN1* – 9.0.0.1 та *WLAN2* – 11.0.0.1. В даному випадку підключені вузли будуть мати зв'язок з Meraki – сервером.

Для цього треба відкрити роутер і на вкладці *CLI (Command Line Interface)* ввести два програмних коди (табл. 1).

Для **налаштування параметрів пристрою безпеки *Meraki-MX65W*** *(WLAN1)* треба встановити *Laptop* з адаптером бездротової мережі *Linksys-WPC300N* і за допомогою вкладок *Desktop / IP Configuration* увімкнути режим *DHCP* для отримання параметрів: *IPv4 Address* – 192.168.0.2, *Subnet Mask* – 255. 255. 255.0, *Default Gateway* – 192.168.0.1, *DNS Server* – 10.1.1.2. Фіксуємо на вкладці *Config* серійний номер пристрою, наприклад, *0GMT-2P2W-3S34*. Далі відкриваємо вкладку *Desktop* на *Laptop* і у вікно *Web Browser* вводиться IP-адреса 192.168.0.1 *WLAN* пристрою безпеки, а у поле *User Name* – серійний номер (рис. 2). При відкритті пристрою на вкладці *Connection* фіксуємо MAC-адресу пристрою для подальшої

реєстрації на Meraki – сервері, наприклад: *Hardware address* 00:0C:CF:88:A3:52, а на вкладці *Configure* для Internet1 вибираємо у списку режим: *IP assignment – DHCP*. Аналогічним чином встановлюється і налаштовується *Laptop* для *WLAN2* та параметри пристрою безпеки.

Таблиця 1

Програмні коди відкриття служби DHCP

Програмний код для WLAN1	Програмний код для WLAN2
Router(config)#ip dhcp pool Nick Router(dhcp-config)#network 9.0.0.0 255.0.0.0 Router(dhcp-config)#default-router 9.1.1.1 Router(dhcp-config)#dns-server 10.1.1.2	Router(config)#ip dhcp pool Helga Router(dhcp-config)#network 11.0.0.0 255.0.0.0 Router(dhcp-config)#default-router 11.1.1.1 Router(dhcp-config)#dns-server 10.1.1.2

Для **налаштування через хмарний сервер Meraki бездротового зв′язку користувачів та шифрування даних** необхідно у вікні *Web Browser Laptop* ввести https://dashboard.meraki.com, а при відкритті сервера, натиснути кнопку *Create an account* для реєстрації. При цьому і діалогове вікно ввести, наприклад, наступні параметри: *Email*: meraki_admin@cisco.com; *Full name*: *Nick*; *Password*: *12345678*; *Confirm Password*: *12345678*; *Company*: *KTGG*. Натиснути кнопку *Create Account*. Далі з метою створення мереж WLAN1, WLAN2 та реєстрації пристроїв безпеки натискається вгорі посилання *here (тут)* і ліворуч *Create a network*. У поле *Network name* вводиться WLAN1 і натискається кнопка *Create network*. Нижче у відповідні поля вводяться параметри реєстрації пристрою безпеки (серійний номер, MAC-адреса, назва мережі) та натискається кнопка *Add devices*.

Якщо натиснути ліворуч посилання *Security Appliance / Appliance Status / Uplink*, тоді можна побачити стан та конфігурацію інтерфейсу Інтернет порту відповідного пристрою безпеки (рис. 3).

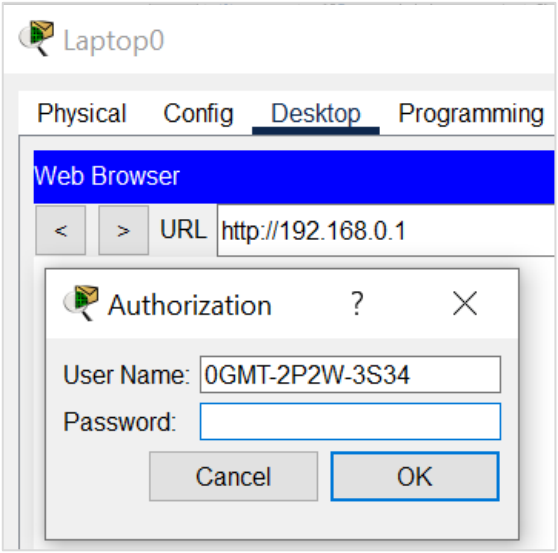

Рис. 2. Авторизація на Meraki-MX65W Security Appliance

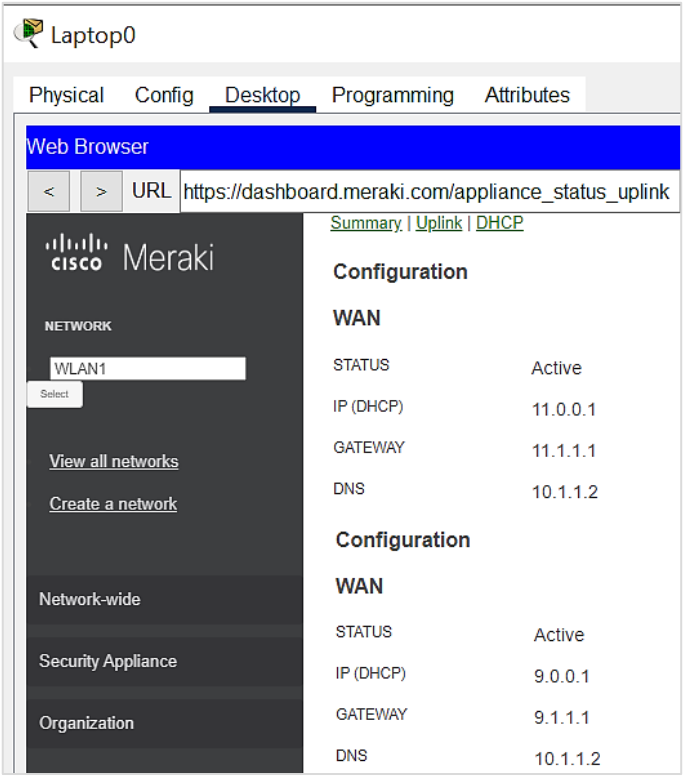

Рис. 3. Сформована на Meraki – сервері конфігурація інтерфейсів Internet-портів підключення вузлів WLAN1 та WLAN2

За посиланням *Security Appliance/ Appliance Setting* здійснюється шифрування доступу вузлів до *WLAN1*, тобто встановлення параметрів: *Status – Enabled, SSID Name – Office1, Security – WPA2 PSK, WPA Key – 1234567890, WPA encryption mode – WPA2 only*.

Натискається кнопка *Save Changes*. Після цього можна до *WLAN1* підключати до 50 вузлів. Аналогічно шифрується доступ до *WLAN2* з визначенням особистого ключа.

Після безпомилкового виконання налаштування параметрів на *Meraki-MX65W Security Appliance* та *Meraki*-сервері буде забезпечена успішна перевірка працездатності підключених вузлів.

Отже, запропонована технологія побудови та захисту бездротових мереж з використанням пристроїв *Meraki* дозволяє вирішити питання посилення безпеки мереж. Представлену технологію можна рекомендувати для використання в навчальному процесі, а також моделювання мереж на стадії проектування.

Список використаної літератури:

1. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі. Навчальний посібник для виконання лабораторних робіт. Київ : НТУУ «Київський політехнічний інститут імені Ігоря Сікорського», 2020. 213 с. URL: http://surl.li/fynzz (дата звернення: 27.03.2023).

2. Налагодження та дослідження роботи CISCO MERAKI. URL: http://surl.li/fvmsb (дата звернення: 27.03.2023).

3. Налаштування бездротової мережі Meraki. URL: http://surl.li/fnedp (дата звернення: 27.03.2023).

4. Скопень М. М., Стародуб О. П. Особливості шифрування та програмування обмеження доступу у бездротових мережах/ Матеріали II Міжнародної наукової конференції на тему «Цифровізація економіки в умовах пандемії: процеси, стратегії, технології» (4–5 лютого 2022 року, Кельце, Польща): Riga, Latvia: "Baltija Publishing". 2022. С. 144–149 URL: http://surl.li/ffcgn (дата звернення 27.03.2023). DOI: https://doi.org/10.30525/978-9934-26-194-7-27.