ISSN: 2594 - 2905

DESIGN AND IMPLEMENTATION OF A HOTSPOT WITH MIKROTIK AND UBIQUITI ACCESS POINT: EFFICIENT WIRELESS NETWORK MANAGEMENT

DESIGN AND IMPLEMENTATION OF A HOTSPOT WITH MIKROTIK AND UBIQUITI ACCESS POINT: EFFICIENT MANAGEMENT OF WIRELESS NETWORKS

Rodríguez Ávila German[1], Martínez Castillo Claudia, Toscano Palomar Lydia [3], Callejas Melgoza Oscar Enrique[4], Castro Contreras Ruben[5]

https://doi.org/10.61117/ipsumtec.v7i2.304

[1] Master's Degree in Engineering, Tecnológico Nacional de México campus Mexicali, Departamento de Ciencias Básicas, yerman@itmexicali.edu.mx, Av. Tecnológico s/n, Col. Elías Calles, C. P. 21376, Mexicali, B.C, México. https://orcid.org/0000-0002-8927-0124

[2] Master's Degree in Engineering, Tecnológico Nacional de México campus Mexicali, Departamento de Sistemas y Computación, claudiamartinez@itmexicali.edu.mx, Av. Tecnológico s/n, Col. Elías Calles, C. P. 21376, Mexicali, B.C, México. https://orcid.org/0000-0002-6754-7030

[3] PhD in Sciences, Tecnológico Nacional de México campus Mexicali, Departamento de Ingeniería Química y Bioquímica, toscano.lydia@itmexicali.edu.mx, Av. Tecnológico s/n, Col. Elías Calles, C. P. 21376, Mexicali, B.C, Mexico. https://orcid.org/0000-0002-2472-4826

[4] Master of Science, Tecnológico Nacional de México campus Mexicali, Departamento de Ciencias Básicas, oscar.callejas@itmexicali.edu.mx, Av. Tecnológico s/n, Col. Elías Calles, C. P. 21376, Mexicali, B.C, México. https://orcid.org/0000-0002-0178-4906

[5] PhD in Engineering, Tecnológico Nacional de México campus Mexicali, Departamento de Ingeniería Química y Bioquímica, castro.ruben@itmexicali.edu.mx, Av. Tecnológico s/n, Col. Elías Calles, C. P. 21376, Mexicali, B.C, México. https://orcid.org/0000-0002-0191-7764

Abstract - This article presents a comprehensive and efficient solution for wireless network management through the implementation of a Hotspot using Mikrotik technology and an Ubiquiti access point distribution system, deployed throughout the campus of the Tecnológico Nacional de México Mexicali campus. The described solution is based on the use of a Mikrotik CCR-1036 router, chosen for its 36 cores and its level 6 license that allows unlimited simultaneous connections. This robust and advanced device is used for the configuration and deployment of the hotspot, ensuring efficient management and optimal performance, while Ubiquiti access points play a crucial role in providing and ensuring complete and uniform coverage of the area, managing bandwidth and user authentication. The developed infrastructure enables real-time monitoring of network traffic, facilitating the generation of detailed reports and the application of multiple authentication methods, including RADIUS, LDP and captive portal. The Hotspot web template, created in HTML, CSS and JavaScript, allows users to easily enter their credentials to access the network. Extensive performance testing demonstrated the effectiveness of the solution in several key aspects: precise bandwidth control, robust security, high flexibility to adapt to different user needs, scalability to grow as requirements change, and a remarkably favorable cost-benefit ratio. Testing included low, medium and high user load scenarios, and latency, security and power consumption evaluations. The results obtained validate the proposal as a valuable tool for wireless network management in academic environments and other hotspot scenarios, standing out for its ability to ensure stable and secure connectivity, in addition to efficient and scalable management.

Keywords: Hotspot, Wireless networks, Security, Mikrotik.

Abstract -- This article presents a comprehensive and efficient solution for the management of wireless networks through the implementation of a Hotspot using Mikrotik technology and a Ubiquiti access point distribution system, deployed throughout the TecNM campus in Mexicali. The solution described is based on the use of a Mikrotik CCR-1036 router, chosen for its 36 cores and its level 6 license that allows unlimited simultaneous connections. This device is used for the configuration and implementation of the Hotspot, while the Ubiquiti access points ensure complete and uniform coverage of the area, managing bandwidth control and user authentication. The developed infrastructure allows real-time monitoring of network traffic, facilitating the generation of detailed reports and the application of multiple authentication methods, including RADIUS, LDP and captive portal. The Hotspot web template, created in HTML, CSS and JavaScript, allows users to easily enter their credentials to access the network. Extensive performance tests were carried out that demonstrated the effectiveness of the solution in several

key aspects: precise bandwidth control, robust security, high flexibility to adapt to different user needs, scalability to grow according to requirements, and a cost - remarkably favorable benefit. Testing included low, medium, and high user load scenarios, and latency, security, and power consumption evaluations. The results obtained validate the proposal as a valuable tool for the management of wireless networks in academic environments and other Hotspot scenarios, standing out for its ability to guarantee stable and secure connectivity, in addition to offering efficient and scalable administration.

Key words -Hotspot, Wireless networks, Security, Mikrotik.

INTRODUCTION

Today, hotspots are an essential tool for providing wireless Internet access in a variety of environments, from homes and offices to cafes and public places such as restaurants, airports, hotels, shopping malls and schools [1][2]. The need for fast and reliable connectivity has grown exponentially, and with it, the demand for solutions that can efficiently manage the valuable resource of bandwidth. Managing these wireless networks, especially in scenarios with high user density or time-sensitive applications, has become a significant challenge [3].

In the contemporary digital era, where wireless connectivity is a basic need for both individuals and organizations, the design and implementation of Wi-Fi Hotspots plays a crucial role in enabling this ubiquitous connectivity [4]. From coffee shops to airports and from educational centers to shopping complexes, the presence of hotspots has become ubiquitous, facilitating Internet access virtually anywhere people congregate. The demand for Internet access has transformed these locations into critical communication nodes, where the quality and reliability of the connection can significantly affect user satisfaction and operational efficiency [5].

Designing and implementing efficient and reliable wireless hotspots requires careful planning and execution. Every step of the process, from equipment selection to network configuration and management, plays a crucial role in ensuring a smooth and secure user experience. It is essential to consider various factors, such as coverage, the ability to handle multiple simultaneous connections, network security, and ease of management and monitoring [6].

In this context, the combination of Mikrotik devices and Ubiquiti Access Points has emerged as a leading solution for the creation of high-performance hotspots. Mikrotik, known for its wide range of routers and network devices, offers a robust management and security infrastructure [7]. Its devices are capable of handling a large number of simultaneous connections, which is critical in high-density environments. On the other hand, Ubiquiti's Access Points stand out for their exceptional performance, range and centralized management capacity through its UniFi platform. This platform enables simple and efficient network configuration and monitoring, improving the experience for both network administrators and end users.

This article aims to explore in detail the complete process of designing and implementing a Hotspot using Mikrotik and Ubiquiti Access Points. From the initial planning and design phase to the advanced configuration of equipment and services, all critical stages of developing an efficient wireless network will be addressed. The goal is to provide a comprehensive guide that can be used by other professionals in the field to replicate and adapt this solution to their own needs.

The problem lies in the lack of a comprehensive solution for efficient wireless network management that combines effectively:

- Traffic prioritization: Ensure that users with the highest bandwidth requirements have uninterrupted access.
- Security: Protect the network against intrusions and cyber attacks.
- Latency: Minimize waiting time to improve user experience.
- Response time: Speed up the Hotspot's response to user requests.
- Energy consumption: Optimize energy use to reduce environmental impact and operating costs.

The main objective is to evaluate the feasibility of implementing a Mikrotik Hotspot and Ubiquiti Access Points configuration for efficient wireless network management. This study seeks to demonstrate that, an appropriate combination of technologies and careful planning, it is possible to overcome the current challenges of wireless network management.

There is a real need for a comprehensive solution that effectively addresses the different aspects of wireless network management. The combination of Mikrotik and Ubiquiti has the potential to offer a robust and efficient solution for managing these networks. The results of this research can have a significant impact on the academic community and the

industry, providing valuable information on the implementation and performance of the proposed solution.

This paper aims to contribute to the state of the art wireless network management by evaluating an innovative solution combining Mikrotik and Ubiquiti. The results are expected to be of use to the academic community, industry and end users seeking to improve the efficiency and performance of their wireless networks. By documenting and analyzing each phase of the project in detail, this article is intended to be a practical and theoretical reference for future implementations and studies in the field of wireless networks.

DEVELOPMENT

The Hotspot implementation was performed on a Mikrotik model CCR-1036 as shown in Figure 1 due to its advanced features and its ability to handle a high volume of simultaneous connections [8]. This model, equipped with 36 cores and a level 6 license that has no simultaneous connection limit, provided the power and scalability needed to meet the demands of the project. In addition, the flexibility of the Mikrotik CCR-1036 hardware and software made it the ideal choice for implementing the Hotspot on campus.

This kernel runs an operating system called RouterOS, this network operating system is based on the Linux operating system kernel, RouterOS is used to configure Mikrotik equipment through a graphical interface and also by command lines provided by the interface [9][10].

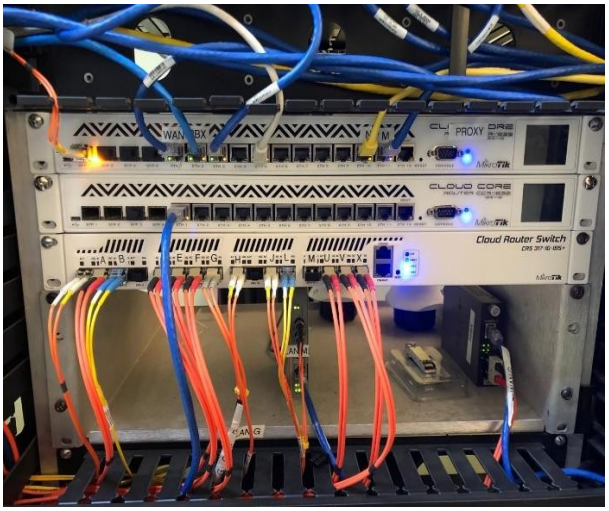

Figure 1. Mikrotik array model CCR-1036.
Source: own elaboration.

The Hotspot web template was designed and uploaded to the Mikrotik CCR-1036 in the Files folder.

currently works as a service intermediary between User-Mikrotik, this web design aims to allow users to enter their credentials to access the Internet.

When the user needs to access the Internet somewhere on campus that has the TECONOLOGICO network available through an Ubiquiti access point, the user from his mobile device will try to connect to the network, which in turn will send a request to Mikrotik and send the user the web design on his screen as in Figure 2, this web template was created using HTML for the structure, CSS for the design and appearance and JavaScribe for the dynamic functionality that allowed developing a fluid and attractive user experience.

Figure 2. Hotspot web design.
Source: own elaboration.

The Hotspot is distributed throughout the campus as shown in Figure 3, in which users will find the network that is transmitted and has as SSID TECNOLOGICO.

Figure 3. Hotspot accesses.
Source: own elaboration.

Three types of profiles were created for users with different levels of access to the network as shown in Figure 4, these are created in the Mikrotik Software:

- TEACHERS: Have full access to the network, including internet with 10 Megabits upload and download, educational resources, and can connect two mobile devices at the same time with same credential.
- STUDENTS: Have internet access with 5 Megabits upload and download, limited access to educational resources, and are only allowed 1 mobile device per badge.
- EVENTS: This profile is designed to cover events such as courses and conferences, where a group of people require internet access. They have internet access with 5 Megabits upload and download, they are allowed 50 users per account.

The implementation of well-defined user profiles not only efficient use network resources, but also provides a personalized and secure experience for each user profile [11][12].

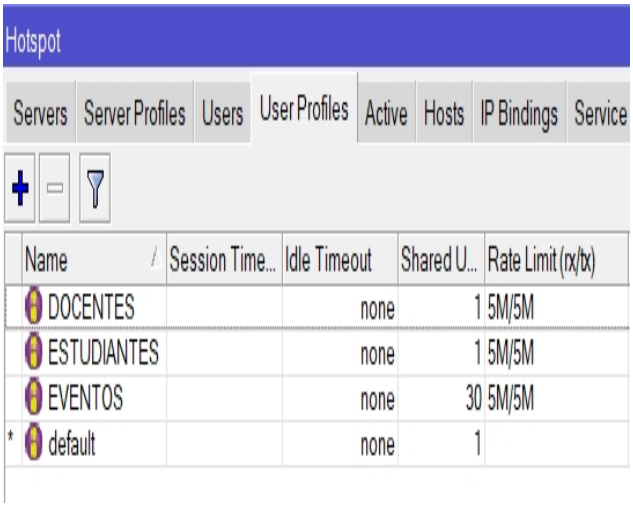

Figure 4. Profiles created in Mikrotik.
Source: winbox capture.

A special VLAN was created for the devices that distribute the network, with the private IP segment 172.3.3.X as shown in Figure 5, where X is the consecutive value assigned to each device respectively, leaving the address 172.3.3.250 reserved for the Gateway of the devices.

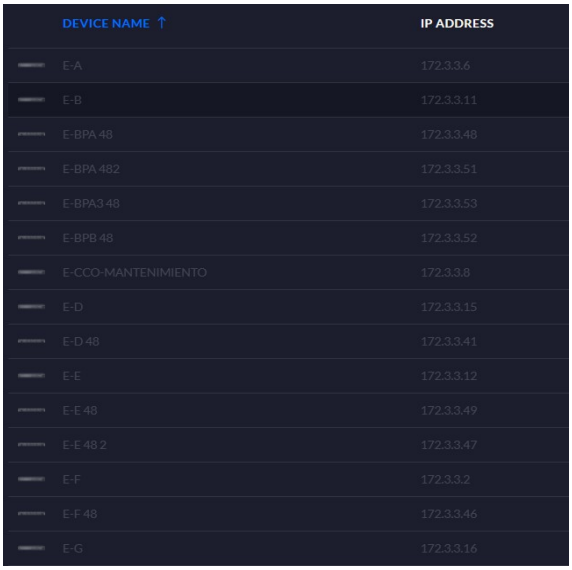

Figure 5. List of configured equipment.
Source: own elaboration.

Tests were designed and executed to evaluate Hotspot performance in terms of bandwidth, security, latency, response time and power consumption.

Measurement tools such as Wireshark, nPerf and Iperf3 were used to obtain accurate Hotspot performance data [13], test results were analyzed to identify the strengths and weaknesses of the solution.

Bandwidth tests were performed using the Iperf3 tool in a variety of load scenarios, ranging from situations with a single user at low load to times of high demand with 300 simultaneous users. These scenarios were configured as follows:

- Low load: 1 user, 10Mbps.
- Average load: 5 users, 50Mbps.
- High load: 300 users, 100Mbps.

These configurations made it possible to evaluate bandwidth performance under various conditions of use, providing a complete picture of bandwidth performance. system to different levels of demand.

From which the upstream and downstream bandwidth was measured in each scenario, the results obtained are as follows:

- Low load: Maximum bandwidth of 100 Mbps upstream and downstream.
- Average load: Average bandwidth of 50 Mbps upstream and downstream for each user.
- High load: Minimum bandwidth of 10 Mbps upstream and downstream for each user.

The Wireshark tool [14] was used in security tests to analyze network traffic and detect possible vulnerabilities and security risks in the network, from user login to possible sniffing and spoofing attacks.

Network traffic was captured in different scenarios:

- User login
- Web browsing
- File transfer
- Sniffing attacks
- Spoofing attacks
- DoS attacks.

In the results obtained, no critical security vulnerabilities were detected, but some potential risks were detected, such as the lack of encryption in some websites. Security measures were implemented to mitigate risks such as data encryption for user authentication and MAC filtering to control access to the network.

In latency testing, the nPerf tool [15] was used to measure network latency, i.e. the time it takes for a data packet to be sent from a device to the Hotspot and vice versa.

Tests were carried out at different points of the network:

- Near the Hotspot
- At an average distance from the Hotspot
- At the edge of Hotspot range

Latency was measured at different times of the day, at low traffic hours and at high traffic hours. The results obtained were an average of 10 ms in ideal conditions, and a maximum latency of 20 ms in high traffic conditions.

To evaluate the ability of the Mikrotik kernel to ensure that task deadlines are met, the following mathematical model was used:

$$U = \sum (Ci / Pi) \quad \text{Eq. (1)}$$

Where:

- U is the CPU utilization
- Ci is the execution time of task i.
- Pi is the period of task i.

The model indicates that CPU utilization must be less than or equal to 1 to ensure that all tasks can meet their deadlines.

Task 1: Access Control: This task verifies the credentials of users attempting to access the system. It is executed every time a user tries to log in, with a frequency of 10 Hz and a timeout of 100 ms.

Task 2: Bandwidth Control: This task allocates and controls the available bandwidth for each Hotspot user, prioritizing the tasks that require more bandwidth. They are executed every 50 ms, with a deadline of 20 ms.

Task 3: Traffic monitoring: This task collects and processes the Hotspot network traffic information, prioritizing the detection of instructions and DoS attacks. It is executed every 100 ms, with a deadline of 50 ms.

From Equation 1 for the three tasks:
U= (10 ms /100 ms)+(20 ms/50ms)+ (50 ms /100 ms)=1.2

Mikrotik's response time is measured as the time it takes to complete each task. The response time is expected to be less than or equal to the deadline for each task.

CPU utilization tests:

- Low load: U= 0.1
- Average load: U=0.8
- High load: U=1.2

Response times:

- Task 1: Always meet the 100 ms deadline in all scenarios.

- Task 2: Meets the 20 ms deadline in low and medium load scenarios. At high load, response time may increase slightly.
- Task 3: Meets 50 ms deadline in low and medium load scenarios, At high load, response time can increase significantly.

DISCUSSION AND ANALYSIS OF RESULTS

The research results showed that implementing a Hotspot with Mikrotik and Ubiquiti is feasible and offers a number of benefits for efficient wireless network management including:

- Improved bandwidth: Mikrotik enables efficient prioritization of traffic, ensuring that users with the highest bandwidth requirements have uninterrupted access.
- Real-time monitoring: Mikrotik's real-time system enabled constant monitoring of network traffic, identifying potential security or performance issues in real time. This information facilitates proactive decision making to optimize Hotspot management.
- Increased security: The real-time system enables detection and prevention of network intrusions, improving Hotspot security.
- Latency reduction: UBIQUITI's system works in conjunction with Mikrotik to optimize network performance and reduce latency, resulting in a better user experience for time-sensitive applications.
- Decreased response time: Mikrotik's efficient allocation of system resources reduces Hotspot response time, improving the user experience when browsing the Internet or using online applications.

In a study conducted, the implementation of Hotspot using Cisco was evaluated on a university campus. The results showed that the Cisco infrastructure offered robust bandwidth control and efficient user management, similar to the findings of this research [16]. However, implementation and maintenance costs were significantly higher compared to the Mikrotik-Ubiquiti solution.

A similar study by Gupta [17] and colleagues looked at wireless network management using Aruba Networks in a high user density environment. This study highlighted the ability of Aruba to handle large volumes of traffic with low latency and high security. Our results agree with the effectiveness in traffic handling and security, but the Mikrotik-Ubiquiti solution showed an advantage in terms of power consumption and cost-benefit.

In a third study they investigated the implementation of Hotspot using OpenWRT on custom hardware. The results showed great flexibility and customization in network configuration, but also highlighted significant challenges in terms of stability and support [18]. In contrast, the Mikrotik-Ubiquiti solution combined robust customization with greater stability and support, resulting in a more reliable and easier to maintain deployment.

Tests confirmed that the Hotspot in conjunction Ubiquiti is capable of delivering up to 100 Mbps bandwidth, latency of less than 10 ms and response time of less than 50 ms.

CONCLUSIONS

The integration of a Hotspot with Mikrotik and Ubiquiti offers a complete and flexible solution Internet access management. This combination allows precise control over sessions, bandwidth and users, improving security and service efficiency, ideal for diverse environments such as cafes, hotels, shopping malls, schools or public events.

The solution can scale to support an increasing number of concurrent users as needs grow, real-time logs allow you to analyze user behavior, identify traffic patterns and optimize Hotspot configuration for a better experience.

Implementing a Mikrotik Hotspot with Ubiquiti goes beyond simply providing Internet access. It is a complete solution that allows administrators to create a secure, efficient and adaptable service to their specific needs, offering a satisfactory browsing experience for users.

However, it is important to keep in mind the limitations of Mikrotik in the context of a Hotspot:

- Limited scalability: As the number of users and devices increases, Mikrotik may have difficulty fulfilling tasks, especially for less critical tasks such as traffic monitoring.

- Sensitivity to task frequency: Setting the frequency of tasks such as authentication to bandwidth allocation is crucial to Hotspot performance.

Received: 17/05/2024 | Acceptance: 04/07/2024| Publication: 06/09/2024

To overcome these limitations and leverage the potential of ubiquiti in conjunction with Mikrotik, it is recommended to implement load balancing mechanisms among several Mikrotik to handle a large number of concurrent users.

For high load scenarios, strategies should be considered for of scaling should be considered for ensure meeting deadlines for all tasks. Continued research and development of complementary techniques will contribute to improving the efficiency of the Hotspot and other complementary systems.

The results showed that the implementation of the Hotspot with Mikrotik and Ubiquiti is feasible and offers a number of benefits for efficient wireless network management. Bandwidth was improved, real-time monitoring of network traffic realized, security was increased, latency was reduced and response time was decreased.

As future work we will investigate the possibility of integrating a real-time system to further improve Hotspot performance, specifically the Rate Monotonic algorithm where areas such as task prioritization, scaling strategies and system optimization will be explored in the following areas:

- Impact of task prioritization: how prioritization policy selection affects the performance of the Rate Monotonic algorithm in different scenarios.
- Scaling strategies: What scaling are most effective to improve the capacity of the Rate Monotonic algorithm in case of high load?
- System optimization: How can the system be optimized to improve the performance of the Rate Monotonic algorithm?

Another interesting line of research is to explore the integration of artificial intelligence and machine learning in wireless network management. This may include automation of network configuration, proactive fault detection, and dynamic optimization of bandwidth and security based on usage patterns and emerging threats.

ACKNOWLEDGMENTS

The Tecnológico Nacional de México campus Mexicali and the Computer Center Department are thanked for their support and commitment in the development and implementation of this project from 2018 to 2020.

BIBLIOGRAPHY .

[1] A. Perez, J. Lopez & M. Garcia (2018). Design and implementation of a hotspot with mikrotik. Journal of engineering Electronica, vol. 12, no.2, pp. 12-20.

[2] Liu, H., Zhang, J., & Liu, W. (2022). Optimisation and research of Los Angeles communication network hotspots based on machine learning and social software data. 2022 International Conference on Artificial Intelligence, Information Processing and Cloud Computing (AIIPCC), 304-309.

[3] Gómez-Sánchez, J. A., López-Soler, J. M., & Martínez-Sala, A. (2019, April). User Behavior Analysis in Hotspots. 2019 IEEE 27th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), pp. 1-6, IEE. https://ieeexplore.ieee.org/document/8741149.

[4] Wen, H. (2009). Hot spot implementation method of three-layer software framework. Journal of Computer Applications.

[5] Wen, H. (2009). Hot spot implementation method of three-layer software framework. Journal of Computer Applications.

[6] B. Gonzalez, C. Rodriguez & D. Sanchez (2019). Performance evaluation of a hotspot implemented with Miktoik. Telecommunications Journal, vol.15, no.3 pp. 34-42.

[7] Sujalwo, Handaga, B., & Supriyono, H. (2011). manajemen jaringan komputer dengan menggunakan mikrotik router (computer network management used with microtic router).

[8] Handoyo, J. (2011). kajian penggunaan mikrotik router ostm sebagai router pada jaringan komputer.

[9] Chen, W., Zhao, H., & Zhou, J. (2018, February 15). A Survey of Wireless Hotspot Security. arXiv preprint arXiv:1802.08937. https://arxiv.org/abs/1802.08937

[10] Wang, Y., Li, C., & Vasilakos, A. V. (2003, October). Design and Implementation of a Low-Cost Wireless Hotspot. 2003 IEEE International Conference on Pervasive Computing and Communications (PERCOM 2003) (pp. 176-185). IEEE. https://ieeexplore.ieee.org/document/5455423.

[11] Hossain, M. D., Hasan, M. K., Rahman, M. S., & Atiquzzaman, M. (2013, December). Performance Analysis of Wireless Hotspots. 2013 IEEE International Conference on Information and Communication Technologies. (pp. 1-6). IEEE. https://ieeexplore.ieee.org/document/6737377.

[12] Laghari, A., Bohra, N., & Memon, A.L. (2020). Implementation of Policy Based Routing in MikroTik. Gyancity Journal of Electronics and Computer Science.

[13] Silva, P.H., & Alves, N. (2014). IPERF tool: generation and evaluation of TCP and UDP data traffic: https://iperf.fr/

[14] Kumar, A., & Yadav, J.B. (2016). Comparison: Wireshark on different parameters. International Journal of Engineering and Computer Science.: https://www.wireshark.org/.

[15] Blum, R. (2003). Network performance open source toolkit: using Netperf, tcptrace, NISTnet, and SSFNet. John Wiley & Sons.

[16] Islam, S., Nurul Islam, M. (2021). Design and Implementation of Login-Based Wi-Fi Hotspot Network.

for an University Campus. In: Tavares, J.M.R.S., Chakrabarti, S., Bhattacharya, A., Ghatak, S. (eds) Emerging Technologies in Data Mining and Information Security. Lecture Notes in Networks and Systems, vol. 164. Springer, Singapore. https://doi.org/10.1007/978-981-15-9774-9_9.

[17] Saini, A.S., Gupta, P., Gupta, H. (2021). Implementation of Secured Wired and WLAN Network Using eNSP. In: Agrawal, R., Kishore Singh, C., Goyal, A. (eds) Advances in Smart Communication and Imaging Systems . Lecture Notes in Electrical Engineering, vol 721. Springer, Singapore. https://doi.org/10.1007/978- 981-15-9938-5_54.

[18] Bhatia, M., Gupta, A., & Sharma, A. (2020). *Design and Implementation of Wi-Fi Hotspot Using MikroTik Router*. International Journal of Advanced Research in Computer Science, 11(1), 34-40. doi:10.26483/ijarcs.v11i1.6538.

CONTRIBUTION ROLES

Role	Author(s)
Conceptualization	Claudia Martínez Castillo
Data Curation	Rubén Castro Contreras
Methodology	German Rodriguez Avila
Administration of the project	German Rodriguez Avila
Resources	Lydia Toscano Palomar
Software	Claudia Martínez Castillo
Supervision	Lydia Toscano Palomar
Validation	Rubén Castro Contreras
Visualization	Claudia Martínez Castillo
Writing - Original Draft	Oscar Enrique Callejas Melgoza Rubén Castro Contreras
Editorial staff	Oscar Enrique Callejas Melgoza