Journal of Applied Research and Technology

www.jart.icat.unam.mx

Journal of Applied Research and Technology 22 (2024) 479-487

Original

Implementation of a remote laboratory focused on the development of industrial automation practices

L. Chuquimarca* • W. Torres • J. Sánchez • L. Amaya

Universidad Estatal Península de Santa Elena, La Libertad, Ecuador

Received 12 04 2023; accepted 06 05 2024
Available 08 31 2024

Abstract: The article explores the use of telecommunications applications in the context of the COVID-19 pandemic, affecting employment and education. Technical fields like electronics and automation faced significant challenges as students required access to critical laboratories for firsthand learning. In answer, the proposal to establish a remote laboratory focused on industrial automation emerged. This initiative aims to complement the academic pursuits of students and educators in electronics and automation. The project utilizes advanced networking technologies such as VPN and RDP to provide students with controlled and secure access to fully equipped workstations, including computers, programmable automation controllers, variable frequency drives, HMI, and other essential devices for firsthand exercises. The article details the architecture and implementation of the remote laboratory and offers a comprehensive overview of remotely conducted firsthand activities. This innovative approach ensures equitable access to high-quality education and prepares students for an ever-evolving professional landscape.

Keywords: Remote, laboratory, industrial, automation

*Corresponding author.
E-mail address: lchuquimarca@upse.edu.ec (L. Chuquimarca).
Peer Review under the responsibility of Universidad Nacional Autónoma de México.

1. Introduction

Currently, the hybrid education model has gained significant popularity, due to the convenience it offers by allowing students to attend classes without having to travel to an educational institution. Since the onset of the COVID-19 pandemic, we have witnessed a fundamental change in our communication and daily activities, leading to the widespread adoption of a lifestyle in which the digital world and internet connectivity have become essential (Gamage et al., 2022). In the university setting, advances in information and communication technologies (ICT) and advanced networking equipment have revolutionized higher education, addressing the challenges of firsthand teaching through innovative approaches such as augmented reality, virtual reality, and remote laboratories, thereby providing new and enriching alternatives for student learning (Raes, 2022).

To train students with a solid knowledge of automation, the State University of the Peninsula of Santa Elena (UPSE) has a dedicated physical space for conducting laboratory exercises with programmable logic controllers (PLCs), human-machine interfaces (HMIs), variable frequency drives (VFDs) and similar resources. These laboratory facilities are essential for students to experiment with and apply techniques related to modern technologies through firsthand assignments, thereby enhancing their learning within the Electronics and Automation Engineering program. However, a significant limitation is that current laboratory equipment can only be used in person, preventing students from accessing these resources virtually or remotely (Dietz et al., 2021). Considering these constraints, it is imperative to investigate potential avenues for virtualization and remote access to these resources to enhance the educational experience of students engaged in automation studies.

The overarching aim of this research is to craft an exhaustive system comprising both hardware and software components. The crux of the project lies in the development of a sophisticated web application tailored to grant educators and students seamless remote access to the automation laboratory's internal network. This access empowers them to fully harness the resources and modules nestled within this environment, as underscored by Aydogmus and Aydogmus (2008). At the heart of this initiative is the strategic utilization of the MikroTik Router's automation capabilities, further fortified by capitalizing on the robust features of a range of open-source software solutions, including Linux, OpenVPN, MariaDB, Hypertext Preprocessor (PHP), and the MikroTik API. Through the meticulous amalgamation of these tools, the project culminates in the genesis of a dynamic web application interface, as eloquently detailed by Islami et al. (2020). This interface not only streamlines user management but also empowers the scheduling of sessions and facilitates seamless workstation access, thereby cultivating an environment ripe for heightened collaboration and productivity.

The primary objective of this project is to address the growing demand for conducting laboratory practices remotely, thereby eliminating the necessity for physical presence. This objective will be achieved through the implementation of a meticulously designed comprehensive system, which encompasses the following pivotal components:

1) A web application.
2) Web client/server infrastructure.
3) Robust network infrastructure.
4) Hardware and software designed for equipment management and protection.
5) Practice guides tailored for programming with programmable logic controllers (PLCs).

These essential elements will form the system's foundation that enables remote access to the laboratory. Communication between end users and the laboratory's internal network, where the practices will occur, will be established using the OpenVPN protocol provided by RouterOS. Subsequently, the Remote Desktop Protocol (RDP) will facilitate remote connection to the application server, where PLC programming will be conducted. This innovative approach not only overcomes geographical barriers but also enhances the efficiency and accessibility of laboratory practices, improving the educational experience for teachers and students in industrial automation.

In educational settings where physical classroom attendance is impractical or when the duration of laboratory activities exceeds constraints, two alternative approaches emerge: Virtual laboratories (VL) and remote laboratories (RL) (Alkhaldi et al., 2016; Hernández de Menéndez et al., 2019; Potkonjak et al., 2016). Virtual laboratories (VLs) simulate real-life scenarios using specialized software, allowing for practical exercises under specific conditions. Conversely, RLs enable students to engage in firsthand experiments within a physical laboratory situated remotely, accessible, and controllable via the internet. Both options play pivotal roles in education, offering flexible and effective solutions where physical presence or direct access to lab equipment may be challenging. This diversity of approaches enriches the learning process, providing students with varied opportunities to cultivate practical skills and knowledge. The proliferation of remote laboratories parallels technological advancements, as evidenced by a study conducted between 2004 and 2006 in Germany. The study aimed to assess the global prevalence of remote laboratories and revealed a substantial increase in their numbers. In 2004, 70 operational remote laboratories were identified, a figure that surged to 120 by 2006, all equipped for remote access and control (Andujar et al., 2010).

This surge underscores the mounting interest in and adoption of remote laboratory technology in educational and research spheres, emphasizing their pivotal role in democratizing access to laboratory practices regardless of geographical boundaries.

On a global scale, distinct types of remote laboratories have emerged, primarily focused on instructing subjects related to engineering. An outstanding example is the Tecnológico de Monterrey, which has implemented three distinct platforms to support its distance education programs (Miranda et al., 2021):

1) MOOC lab serves as a public and massively used laboratory specializing in circuits and electrical measurements, equipped with ten workstations accommodating over 1600 weekly sessions for students.

2) eLab/TeleLab is a virtual environment dedicated to electrical, electronic, and mechatronic engineering, encompassing areas such as instrumentation, electrical circuits, electronics, and electrical machines, as well as automation, industrial networks, robotics, and control.

3) The remote labs platform has been exclusively designed for researchers and graduate students, providing a specialized space for experimentation in power theories, power electronics, motors, and electrical generators.

These platforms reflect the institution's commitment to high-quality education and promoting advanced technical and scientific research fields.

The remarkable success of these laboratories has led to the development of remote access to laboratories from any computer in the world. This is made possible by the requirement of an internet connection. One such company is LabsLand, which offers remote experimental learning using real laboratories. The range of learning possibilities extends from physics and kinematics laboratories to specialized laboratories in radioactivity. This pioneering approach democratizes access to innovative laboratory resources and significantly expands opportunities for experimental learning, thereby opening new perspectives for education and research in an increasingly digitally connected world (Achuthan et al., 2021; Orduña et al., 2018).

In the realm of educational and research endeavors, remote laboratories share a common reliance on payment or subscription models to grant full access, which is pivotal for ensuring their economic sustainability. Notably, certain laboratories extend limited access through free trial periods, while exclusive privileges are reserved for members of select educational institutions actively engaged in developing these remote facilities. This economic framework underscores the paramount importance and perceived value of remote laboratories. It empowers institutions and service providers to consistently uphold and enhance the quality and functionality of these indispensable resources. The research methodology employed in this study encompassed various stages, including the development of the proposal, the execution of the project, and the analysis of research results. The "research methods" section outlines the methodologies and approaches used to gather data and conduct experiments. In "development of the proposal," the initial project framework, objectives, and methodologies were detailed. "Research results" presents the findings and outcomes of the study, highlighting the data and insights obtained. Finally, the "conclusions" section summarizes the key takeaways and implications derived from the research, providing a comprehensive understanding of the study's outcomes.

2. Research methods

This section will provide an in-depth exploration of the design of the remote laboratory system's various components. It will delve into creating the internal laboratory network diagram, finalizing the infrastructure configuration of the scheduling system, and addressing critical aspects related to electrical safeguards at each stage of analysis. Through this comprehensive design review, readers will gain a thorough understanding of the conception and development of the remote laboratory system. This will underscore its strength and ability to deliver a secure and efficient learning and experimentation experience.

2.1. Physical network topology

In crafting the physical network design, our installation of a MikroTik Router within the laboratory was a strategic choice. This router was selected for its extensive functionalities, including the ability to establish a virtual private network (VPN) server, generate authentication certificates, feature a built-in security system, and, notably, automate various network operations. Among these operations, noteworthy are computer power management and continuous monitoring of their status, seamlessly facilitated through the Application Programming Interface (API) tailored specifically for PHP. This meticulously configured infrastructure serves as a pivotal component of the overall system, empowering precise control, and effective management of the laboratory network. Such meticulous control is paramount for ensuring an efficient and dependable learning and experimentation environment (refer to Figure 1). The connection of elements belonging to each rack is achieved using an unmanaged TP-Link switch, which, in turn, connects to the Hewlett Packard Enterprise (HPE) switch that distributes the network throughout the laboratory, enabling communication between each element and the MikroTik Router. It is essential to highlight that the web server is connected through a bridge interface to the laboratory's external network. This means that both the router and the server are in the same network segment, resulting in the ability

to access the web application and the MikroTik Router through any public IP address assigned by the institution's IT department, emphasizing the consistency and comprehensive accessibility of the implemented network infrastructure.

2.2. Logical network topology

Once all the physical network connections are in place, the next step involves the logical design, where the various network devices are configured with logical addresses Internet Protocol (IP) to ensure they are unique and do not overlap. Furthermore, all IP addresses are assigned within the same network segment, resulting in seamless communication among the network elements. This logical design process is crucial for establishing a coherent and efficient network structure, ensuring that each device can be appropriately identified and accessed within the laboratory environment.

2.3. Communication rack

The communications rack consists of two network devices and a computer running the Ubuntu Server operating system, serving as a web and database server. The network devices include a MikroTik RB2011 UiAS-2HnD-IN router and an HPE OfficeConnect 1920 24G switch. The communications rack, its components, and its electrical protection power strip are depicted in Figure 2. This configuration is essential for the comprehensive operation of the remote laboratory system, enabling effective network management and ensuring a secure and reliable environment for learning and experimentation.

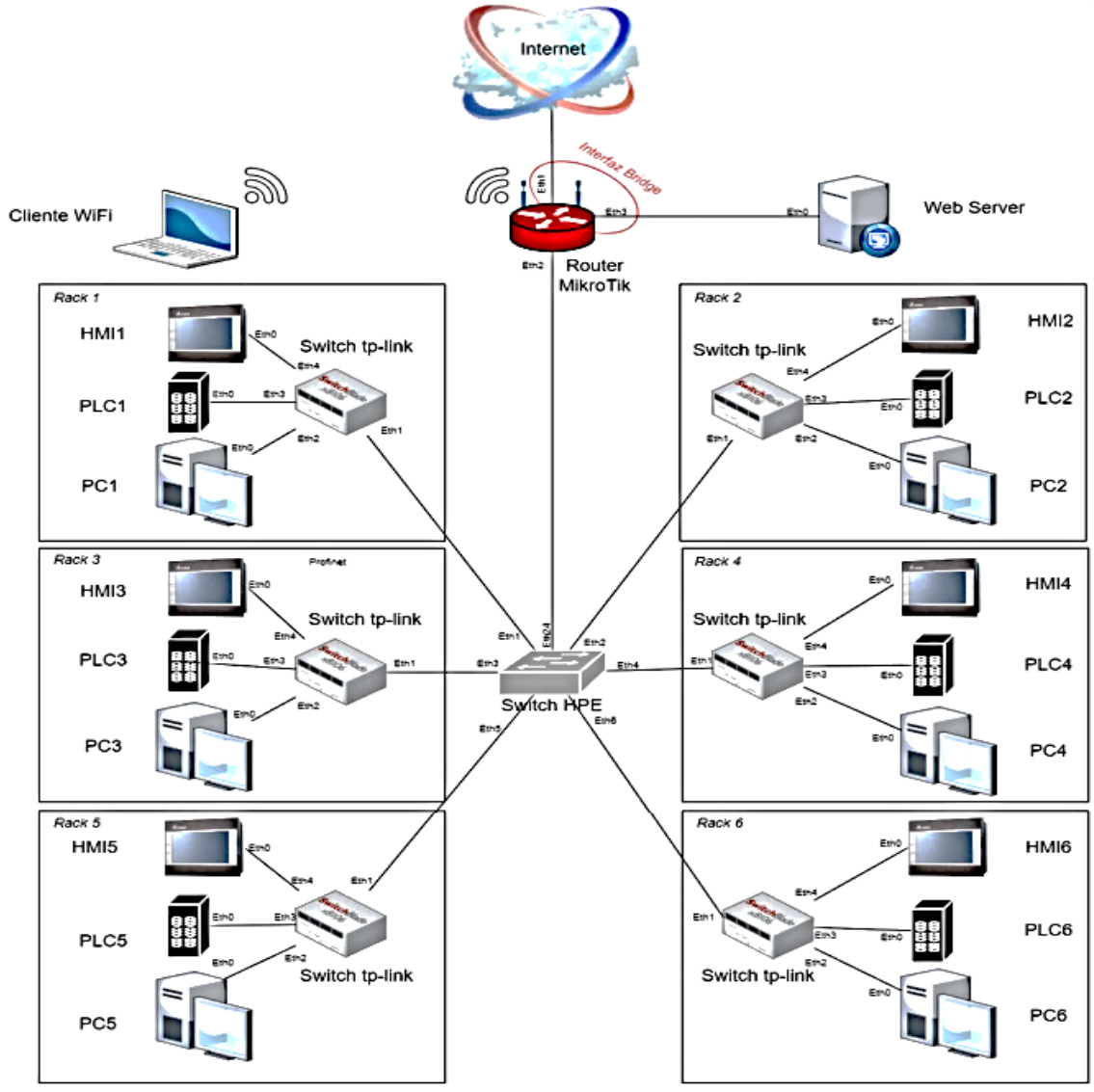

Figure 1. Physical topology of the laboratory's internal network.

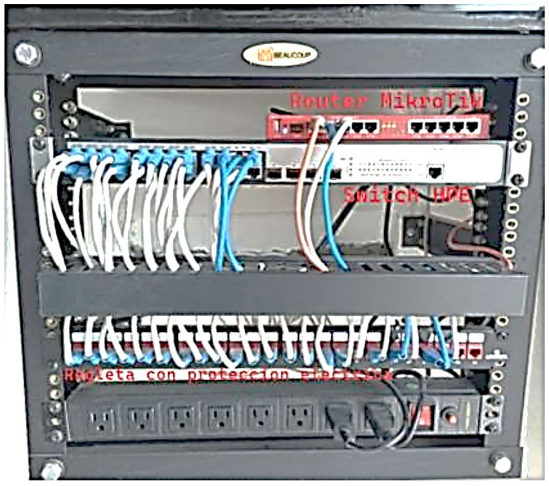

Figure 2. Automation laboratory communications rack.

3. Development of the proposal

Any student or instructor needing remote access to equipment within the automation laboratory requires a secure connection method to prevent data interception by malicious third parties. Therefore, the following section outlines the measures implemented in the project to ensure the security of user data.

3.1. VPN design

For a student to remotely access the physical resources of the laboratory, they will need to use the OpenVPN application. First, a comprehensive design is required to understand the operation and mode of operation of the VPN, analyzing from the moment a student wishes to conduct a practice from their home or any other location external to the university to their connection to the computer where they will perform the practice with the laboratory's elements. The diagram representing this process can be seen in Figure 3.

As seen in Figure 3, a remote client can access a private network using a VPN. In the specific case of the UPSE automation laboratory, the MikroTik Router serves as the OpenVPN server, housing the certificates required for student access to the laboratory and providing an additional layer of security by encrypting data through a VPN tunnel. To connect with the VPN from a location external to the laboratory, the student must possess a digitally signed certificate from the VPN server and unique access credentials. All this information must be entered into the OpenVPN client installed on their computer for a valid connection. The annex will explain specific details about the remote client connection process later. Once the VPN connection is successfully established, and if the remote client has made a prior reservation through the web scheduling application, the process proceeds with an RDP connection to the reserved computer.

3.2. Design and implementation of OpenVPN on MIKROTIK Router

To perform the functional tests of the OpenVPN protocol on a MikroTik Router, a test environment has been created simulating the computers within the automation laboratory and a remote user equipped with a Windows operating system device to verify the connection to the internal laboratory elements. The network design was developed using GNS3 due to its ability to emulate real system images such as RouterOS and Windows, and the network diagram is shown in Figure 4. This configuration allows for the evaluation and validation of the OpenVPN protocol's functionality in a controlled environment before its implementation in the production environment of the automation laboratory.

In Figure 4, we can identify three elements briefly:

1. The first element is the laboratory network, which extends from the MikroTik Router at the top to the client PCs at the bottom. Only two computers, PC5 and PC6, are used for this test.

2. The second element is the router named 'internet,' which simulates all the routing from the external network to the university, connecting the remote client's public IP with the laboratory's public IP.

3. The final component encompasses the client's network, comprising a router and a switch. In a practical scenario, these components would typically be consolidated into a single device capable of performing both functions, such as a router/switch utilized by Internet service providers or an Optical Network Unit (ONU) for residential fiber optic service (FTTH). Furthermore, the setup includes two computers, with one running a Windows operating system designated for the subsequent installation of the OpenVPN client and functionality testing.

After enabling all routing functions, it is crucial to emphasize that connectivity relies exclusively on public IP addresses, as private networks cannot establish direct connections. This limitation arises from two main factors. Firstly, private networks require routing at the level of internet service providers. Secondly, these networks connect to the internet via a router utilizing Network Address Translation (NAT) mechanisms.

The results of connectivity tests conducted using the Internet Control Message Protocol (ICMP) from a Windows computer, targeting both the public IP of the MikroTik Router and a PC within the laboratory network, are detailed below. The results obtained in this test are as expected, as the only successful response comes from the public IP address. The remote host cannot reach that destination since the private IP address is not routed to the internet.

A VPN is required to enable a host to establish connectivity with a remote private network. Below are the steps for setting

up an OpenVPN server within a MikroTik Router. Initially, connect to the MikroTik Router using the WinBox application. As the first step, generate certificates for both the server and the clients.

In conclusion, we need to generate client certificates. It is imperative to understand that our testing environment involves a virtualized MikroTik Router without a license, limiting us to one VPN client connection at a time. Therefore, we will only be generating one client certificate.

Next, we execute the following line in the router's terminal to sign the CA-TMP certificate and rename it as CA. Now that we have the certificate authority adequately signed, we proceed to sign the SERVER certificate with this entity. Finally, we perform the signing of the client certificate.

In the realm of user authentication, it is pivotal to set up credentials, a process undertaken within the secrets section. Here, the input of both username and password is paramount. Additionally, within this tab, selecting the client's service type as OpenVPN and opting for the "default-encryption" encryption profile are critical steps. Lastly, we assign the default virtual IP address "10.0.0.1" to the VPN server, while designating the remote client's IP as "10.0.0.11".

Moreover, to enable the OpenVPN client to establish a remote connection, it is imperative to export the certificates. This process involves selecting the certifying authority "CA" and right-clicking to access the options menu. From there, choose "export" to proceed with the exportation of the certificates.

3.3. Access control through the embedded firewall in MikroTik

With all the steps completed, we now have an active VPN server with access credentials for remote clients. Next, we will implement access control using the embedded firewall provided by MikroTik's RouterOS operating system. To provide access control for organized laboratory use, we intend to manage each remote client's access time and date using MikroTik's firewall capabilities.

To efficiently manage remote clients within our system, we will compile an access list using the virtual IP addresses assigned to each client, based on our predefined network segment for remote access. Initially, we will implement a general firewall rule that blocks access for all clients within this segment. Access will then be granted exclusively to the remote client who has scheduled a session in advance. This strategy ensures secure and controlled access, thereby maintaining the system's integrity and operational efficiency.

Subsequently, to establish the general rule for blocking all VPN clients from accessing the internal network, a new firewall rule is created, with the setting that all traffic will be denied (dropped). Furthermore, the configurations create the rule that allows access (accept) to a single remote client, and this client, in turn, will have access only to a single host within the laboratory. An essential aspect to consider is that firewall rules have a priority level based on their position within the list. In other words, if we place the general blocking rule first and then allow access to a specific client below it, the remote client will not be able to access the internal resources of the laboratory. Therefore, caution must be exercised when creating firewall rules. One of the advantages of the MikroTik graphical interface is that changing the position of a rule is as simple as dragging it up or down. Moreover, rules can be moved using the command line via SSH or Telnet, offering flexibility not found in brands like CISCO.

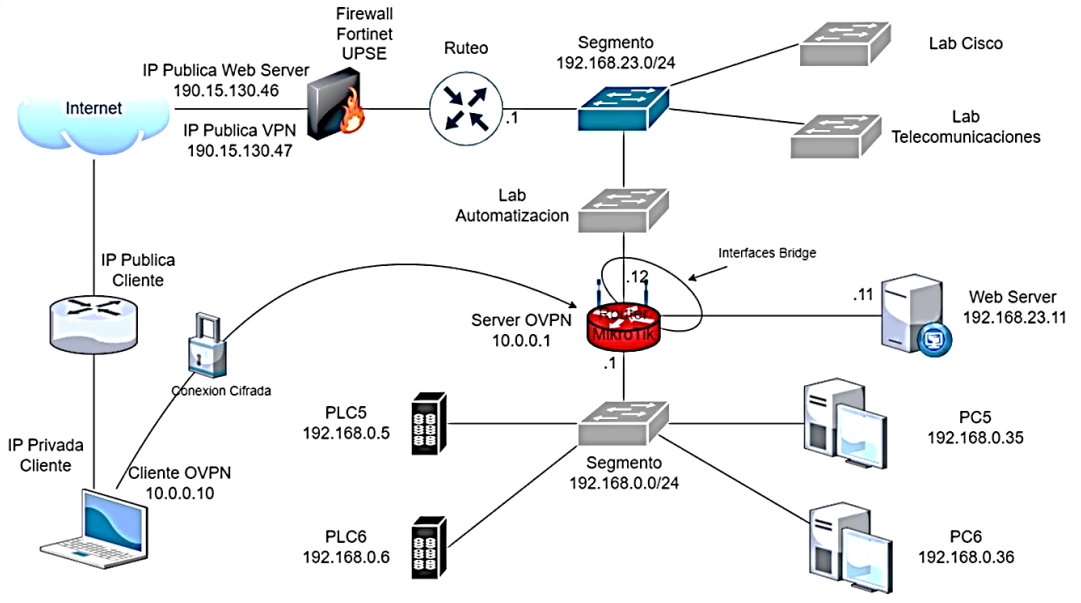

Figure 3. Topological design of the VPN network

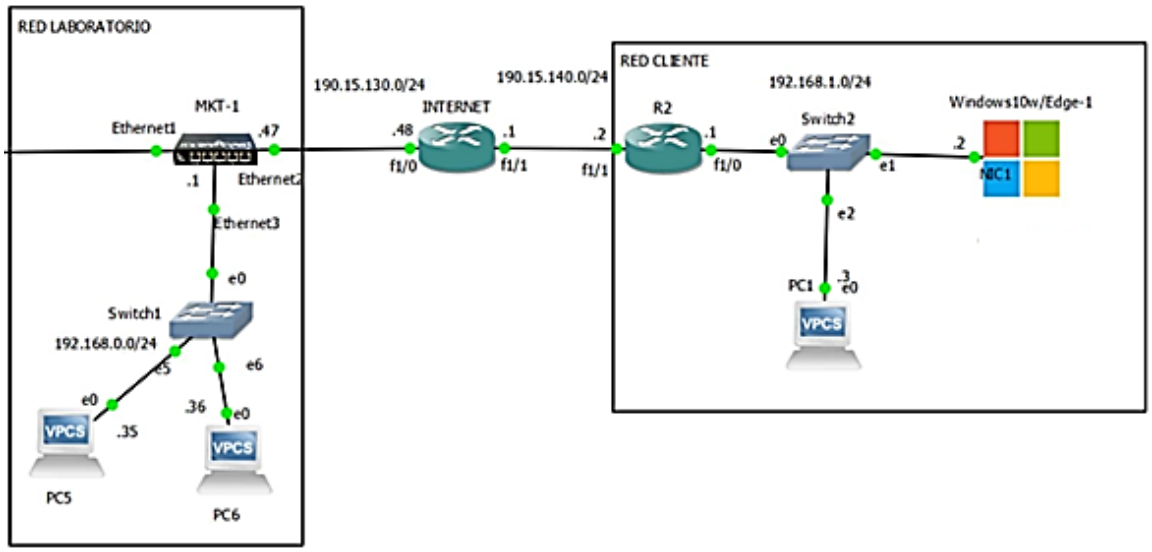

Figure 4. Network design for testing.

4. Research result

As an initial evaluation point, we verified that the teacher or system administrator could check the status of powered-on PLCs through the web application and remotely power on the computers. The results indicate that only two PLCs were powered on, as denoted by the green indicators, while no computers were powered on.

The monitor of PC-6 displayed the characteristic TIA Portal image, confirming that the PC was powered on and that the remote power-on function was operating correctly. To further evaluate the system's capabilities, we enlisted the assistance of two students. Each student scheduled a session for the same date and time on different PCs within the laboratory. This simultaneous usage was designed to rigorously assess the system for potential latency issues or excessive resource consumption, ensuring its robustness and efficiency under real-world conditions.

Simultaneously, the web server communicates via the RouterOS API to schedule student access to the internal laboratory hosts. To achieve this, it creates two schedulers for each appointment: one to grant access and the other to revoke it.

To schedule appointments correctly in MikroTik, a total of five instructions must be executed. First, create a firewall rule allowing access from the remote VPN IP to the local PC's IP intended for connection. Next, position this rule above another rule blocking access from all other remote IPs. Since firewall rules in MikroTik are enabled by default, the following step involves deactivating the rule. This allows for later activation and removal by the two schedulers created at the end.

All of this can be observed in the RouterOS Log using WinBox. Suppose we navigate to the firewall rules in WinBox. In that case, we can observe the two generated rules temporarily disabled and positioned above the general rule for blocking all IPs assigned to remote students. By examining the Log window in conjunction with the firewall window, it becomes evident that at the scheduled time, both rules were enabled, allowing remote students access.

Finally, after the session concludes, the cleanup scheduler fulfills its purpose by removing the firewall rule that blocks access for the respective student. It also removes the schedulers created during the scheduling process, thus preventing residual files from congesting the router's memory.

When the firewall rule allowing access is active, the student can connect to the VPN and gain access to the laboratory's internal network. Subsequently, they can connect via the RDP protocol to the PC assigned to them within the laboratory to conduct the practice assigned by the instructor. Figure 5 illustrates the steps taken by MikroTik to authenticate the remote connection's validity. Also, it displays the IP assigned through the VPN, which is used for controlled access to the laboratory.

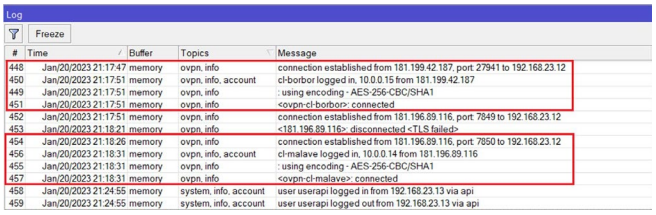

Figure 5. Log of the remote connection via OpenVPN.

In Figure 6, we analyze the data traffic generated by both remote clients simultaneously while using the assigned PC within the laboratory via the RDP protocol. As observed in the above image, the client traffic does not exceed 500 kbps, and the CPU load is well below 50%. Therefore, it can be concluded that the system is operating optimally and ensures that it will not become saturated during its operation.

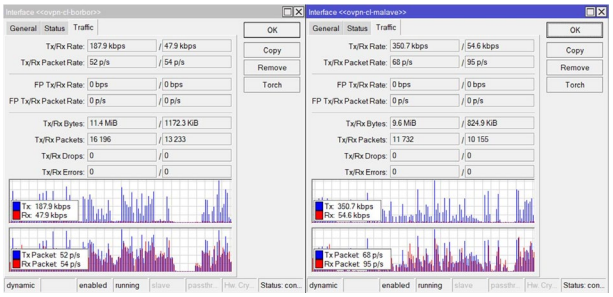

Figure 6. Analysis of data traffic from remote clients.

The initial evaluation of the system's functionality centered on its capacity for remote monitoring and control of powered-on PLCs via the web application. Despite the observation that only two PLCs were powered on while no computers were active at the time, subsequent verification tests validated the successful operation of the remote power-on feature, as evidenced by the TIA Portal image displayed on PC-6's monitor.

To ensure the system's resilience under real-world conditions, a rigorous assessment was conducted by concurrently scheduling sessions on different laboratory PCs by two students. Leveraging the system's communication capabilities with the RouterOS API, the web server efficiently managed access privileges through schedulers, ensuring effective student participation.

In crafting a meticulous process encompassing five instructions, the system outlined a procedure within the MikroTik framework to accurately schedule student appointments and maintain controlled access to laboratory resources. This included the strategic creation, activation, and removal of firewall rules via schedulers, designed to accommodate student access schedules while preserving system efficiency. Analysis of the remote connection process via OpenVPN unveiled MikroTik's robust authentication protocols and IP assignment mechanisms, both critical components ensuring controlled laboratory access.

Furthermore, an in-depth examination of data traffic generated by remote clients utilizing assigned PCs through the RDP protocol showcased the system's optimal performance, with client traffic remaining below 500 kbps and CPU load comfortably below the 50% threshold. These comprehensive findings underscore the system's capacity to operate seamlessly without the risk of saturation, affirming its suitability for sustained and efficient operation in practical laboratory environments.

The relevance of this article lies in its innovative approach to developing a system to support the educational process, specifically tailored for remote execution of laboratory work in industrial automation, with a primary focus on controller programming. The results of the initial tests highlight the system's capability to monitor and control PLCs, as well as remote power on computers, promising significant improvements in the efficiency and accessibility of educational laboratories in remote settings. Additionally, the meticulous description of procedures and the rigorous evaluation involving student participation reinforce the reliability and effectiveness of the system under real-world conditions, substantiating its practical applicability in educational environments.

In terms of contributions, this article presents a detailed and comprehensive methodology for implementing and managing a remote laboratory, offering clear guidelines for scheduling student appointments, and ensuring controlled access to laboratory resources. The integration of technologies such as MikroTik and OpenVPN for remote connection authentication and data traffic management demonstrates a robust and efficient solution to facilitate students' remote interaction with laboratory resources. Furthermore, the performance evaluation reveals that the system operates optimally, without the risk of saturation, underscoring its ability to provide a seamless and effective remote laboratory experience for both students and teachers. These contributions provide a solid framework for the successful design and implementation of remote laboratories in educational settings, thereby enhancing the quality and accessibility of education in industrial automation.

5. Conclusions

Control panels that comply with international regulations were successfully constructed, strictly adhering to established electrical standards in both schematic design and low voltage protection. Additionally, communication components were integrated according to recognized standards such as ANSI/EIA/TIA-568-A, ensuring an efficient wired structure. The establishment of a robust network enabled secure remote access for users via VPNs, utilizing advanced encryption and strong authentication. Furthermore, a real-time monitoring system was implemented using industrial sensors and temperature controllers, guaranteeing precise and timely feedback for actuator control. An innovative remote activation system for PLCs was proposed, leveraging low-power technologies and efficient microprocessors. Interconnection among all components, including PLCs and other devices, was facilitated through a PROFINET-compatible data network, enabling wireless PLC programming via Wi-Fi standards.

Conflict of interest

The authors have no conflict of interest to declare.

Acknowledgements

UPSE – FACSISTEL – CIST.

Funding

The authors received no specific funding for this work.

References

Achuthan, K., Raghavan, D., Shankar, B., Francis, S. P., & Kolil, V. K. (2021). Impact of remote experimentation, interactivity and platform effectiveness on laboratory learning outcomes. *International Journal of Educational Technology in Higher Education*, *18*, 1-24. https://doi.org/10.1186/s41239-021-00272-z

Andujar, J. M., Mejías, A., & Márquez, M. A. (2010). Augmented reality for the improvement of remote laboratories: an augmented remote laboratory. *IEEE transactions on education*, *54*(3), 492-500. https://doi.org/10.1109/TE.2010.2085047

Alkhaldi, T., Pranata, I., & Athauda, R. I. (2016). A review of contemporary virtual and remote laboratory implementations: observations and findings. *Journal of Computers in Education*, *3*, 329-351. https://doi.org/10.1007/s40692-016-0068-z

Aydogmus, Z., & Aydogmus, O. (2008). A web-based remote access laboratory using SCADA. *IEEE Transactions on education*, *52*(1), 126-132. https://doi.org/10.1109/TE.2008.921445

Dietz, M., Abebe, A., Lederer, J., Michl, T., & Schmidt-Vollus, R. (2021). Case study of a virtual lab environment using virtualization technologies and a desktop as a service model. In *Interactive Mobile Communication, Technologies and Learning* (pp. 799-811). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-96296-8_72

Gamage, K. A., Gamage, A., & Dehideniya, S. C. (2022). Online and hybrid teaching and learning: Enhance effective student engagement and experience. *Education Sciences*, *12*(10), 651. https://doi.org/10.3390/educsci12100651

Hernández de Menéndez, M., Vallejo Guevara, A., & Morales-Menendez, R. (2019). Virtual reality laboratories: a review of experiences. *International Journal on Interactive Design and Manufacturing (IJIDeM)*, *13*, 947-966. https://doi.org/10.1007/s12008-019-00558-7

Islami, M. F., Musa, P., & Lamsani, M. (2020). Implementation of Network Automation using Ansible to Configure Routing Protocol in Cisco and Mikrotik Router with Raspberry PI: Array. *Jurnal Ilmiah KOMPUTASI*, *19*(2), 127-134. https://doi.org/10.32409/jikstik.19.2.80

Miranda, J., Navarrete, C., Noguez, J., Molina-Espinosa, J. M., Ramírez-Montoya, M. S., Navarro-Tuch, S. A., ... & Molina, A. (2021). The core components of education 4.0 in higher education: Three case studies in engineering education. *Computers & Electrical Engineering*, *93*, 107278. https://doi.org/10.1016/j.compeleceng.2021.107278

Orduña, P., Rodriguez-Gil, L., Garcia-Zubia, J., Angulo, I., Hernandez, U., & Azcuenaga, E. (2018). Increasing the value of remote laboratory federations through an open sharing platform: LabsLand. In *Online Engineering & Internet of Things: Proceedings of the 14th International Conference on Remote Engineering and Virtual Instrumentation REV 2017, held 15-17 March 2017, Columbia University, New York, USA* (pp. 859-873). Springer International Publishing. https://doi.org/10.1007/978-3-319-64352-6_80

Potkonjak, V., Gardner, M., Callaghan, V., Mattila, P., Guetl, C., Petrović, V. M., & Jovanović, K. (2016). Virtual laboratories for education in science, technology, and engineering: A review. *Computers & Education*, *95*, 309-327. https://doi.org/10.1016/j.compedu.2016.02.002

Raes, A. (2022). Exploring student and teacher experiences in hybrid learning environments: Does presence matter?. *Postdigital Science and Education*, *4*(1), 138-159. https://doi.org/10.1007/s42438-021-00274-0