www.editada.org

International Journal of Combinatorial Optimization Problems and Informatics, 16(2), April 2025, 123-129. ISSN: 2007-1558. https://doi.org/10.61467/2007.1558.2025.v16i1.419

Design and implementation of a wireless network with mechanisms that do not violate security to meet the demand of higher education institutions

Miguel Ángel Ruiz Jaimes [1], Jorge A. Ruiz Vanoye[1], Juan José Flore Sedano[2], Yadira Toledo-Navarro[2]
[1] Polytechnic University of the State of Morelos, Mexico.
[2] Polytechnic University of Pachuca, Mexico
[3] National Center for Research and Technological Development, Mexico.
E-mails: mruiz@upemor.edu.mx

Abstract. At the Autonomous University the current wireless network infrastructure is insufficient to meet the growing demand for access, causing failures and intermittencies in the service. Faced with this problem, a thesis proposal has been developed to implement a modern wireless network with high user density, centralized management and improved security schemes. The proposed methodology for the implementation of a high-density wireless network in a higher education institution. In conclusion, the project made it possible to comply with the hypothesis proposed since the implementation of a robust wireless network, with adequate levels of security and profile management, facilitated the ubiquitous access of online academic resources by the student and teaching community of the university. This translates into support for educational quality.
Keywords: Wireless Network, Higher Education Institutions, Security, High-Density Networks, Centralized Management.

Article Info
Received Dec 26, 2024
Accepted Mar 11, 2025

1 Introduction

At the Autonomous University the current wireless network infrastructure is insufficient to meet the growing demand for access, causing failures and intermittencies in the service. Faced with this problem, a thesis proposal has been developed to implement a modern wireless network with high user density, centralized management and improved security schemes.

- Among the main objectives of the project are:
- Deploy a robust wireless network in the university.
- Create a reference methodology applicable in other Higher Education Institutions.
- Provide access to electronic resources to students through mobile devices.
- Provide teachers with an academic support tool.
- Ensure information integrity through access policies.
- Establish centralized network management.
- Implement proactive monitoring and fault detection.
- Strengthen Security with Two-Factor Authentication

This solution would benefit the approximately 30,000 users among students, teachers and administrative staff of the university, facilitating their seamless access to the university's digital academic resources.

The new wireless network infrastructure represents a significant advance in terms of capacity, stability, security and user experience for the university community. The proposal also incorporates a methodology that could serve as a reference for the implementation of similar networks in other higher education institutions in the country.

2 Theoretical framework

Computer networks originated in 1969 when ARPANET was established (Information Sciences Institute University of Southern California, 1981). Wireless networks, especially Wi-Fi, have advanced greatly, evolving from the 802. 11b standard, which had speeds of 11 Mbps, to the more recent 802. 11ac standard that offers speeds up to 1. 3 Gbps (Izaskun Pellejero, 2006).

The security of wireless networks is a vital concern. The ISO/IEC 27001 standard offers a framework for handling security risks (International Organization for Standardization, 1989). Additionally, the Bring Your Own Device (BYOD) trend is on the rise, demanding effective security measures (Ronald van Kleunen, 2016).

Table 1. Comparison of IEEE 802.11 Wireless Standards

Standard	Description
802.11b	The 802.11 standard is currently the most widely used. It offers a maximum total output of 11 Mpbs (6 Mpbs in practice) and has a range of up to 300 meters in an open space. It uses the 2.4 GHz frequency range with three radio channels available.
802.11g	The 802.11g standard offers high bandwidth (with a maximum total throughput of 54 Mbps but 30 Mpbs in practice) in the 2.4 GHz frequency range. The 802.11g standard is compatible with the previous standard, 802.11b, which means that devices that support the 802.11g standard can also work with 802.11b.
802.11N	The 802.11n standard exists in both the 2.4 GHz: 802.11 b/g/n band, as well as the 5 GHz: 802.11 a/n band. Phased Co-existence Operation (PCO) mode of operation allows 802.11n to dynamically change the operating channel from 40 MHz to 20 MHz with a significant increase in maximum transmission rate from 54 Mbps to a maximum of 600 Mbps
802.11ac	The 802.11ac standard operates only in the 5GHz band where there is less noise and interference from competing technologies. In addition, there is a lot of space available in this band, which allows for an increase in the number of flow channels in this band, as opposed to the three in 802.11n. The standard consists of improving transfer rates up to 433 Mbit/s per data stream, theoretically achieving rates of 1.3 Gbit/s using 3 antennas.

3 Methodology

This study follows an experimental and projective approach to develop and evaluate a wireless network prototype. The MIRIAD methodology includes three stages:

1. Evaluation: Analyzing available technologies and conducting controlled environment tests (Gartner, 2013).
2. Preparation: Designing network topology, configuring authentication, and implementing redundancy (Pablo González, 2015).
3. Follow-up: Deploying the solution, knowledge transfer, optimization, and maintenance (Cano, 2015).

Tools such as Wi-Fi security testing software and network coverage analyzers were employed (Ookla, 2017).

.

Figure 1. MIRIAD methodology for high-density wireless network implementation**.**

4 Design and implementation

Considering what the Autonomous University of the State of Morelos (UAEM) requires, enterprise-grade elements from Extreme Networks were chosen. The network consists of 220 AP3715i access points that are controlled by two V2110 virtual controllers located on a Dell PowerEdge server (Network RADIUS SARL, 2016).

The physical/logical design considers access and core switches for interconnection of the existing wired infrastructure with the new wireless APs. A coverage study was also carried out, defining the location of equipment, channels and frequencies in the 2.4GHz and 5GHz bands to optimize the service.

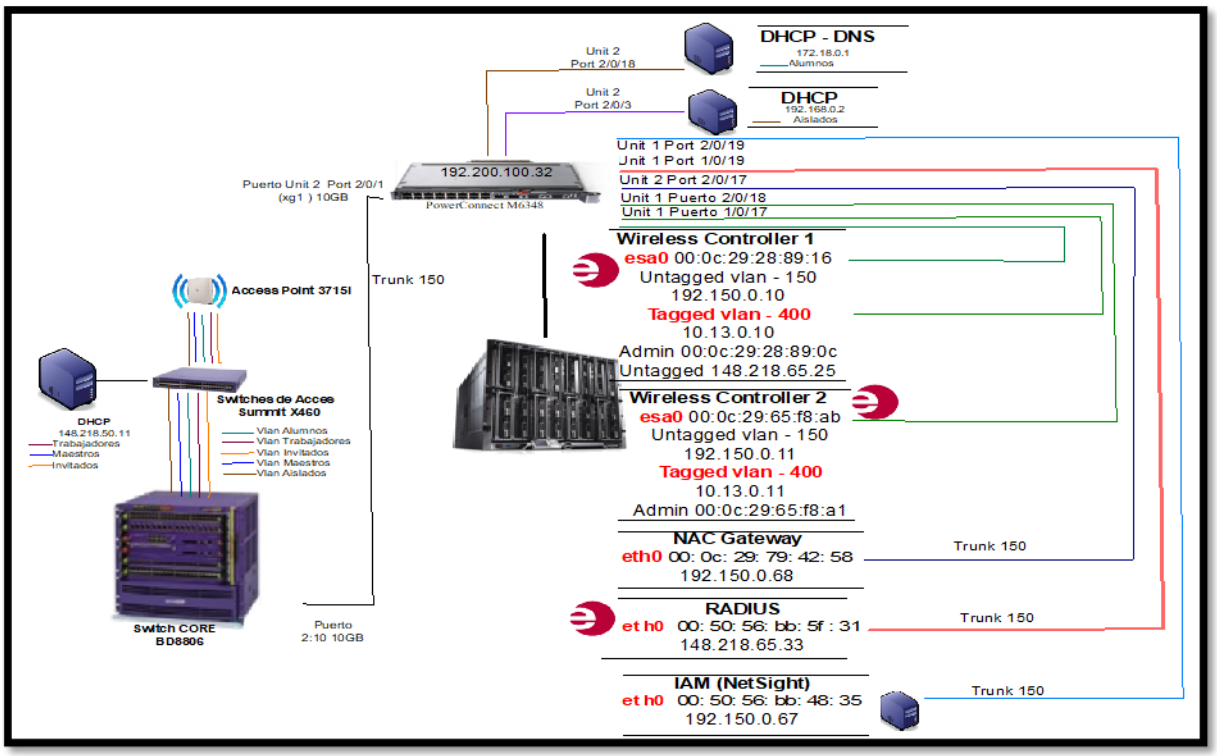

Figure 2. Network topology for high-density wireless deployment.

At the user profile level, roles were established with bandwidth limits and resource access restrictions according to the segment: Students (6 Mbps, academic resources only), Teachers (6 Mbps, no restrictions), Workers (14 Mbps, no restrictions), Guests (2 Mbps, limited access), and Network Administrators (full access).

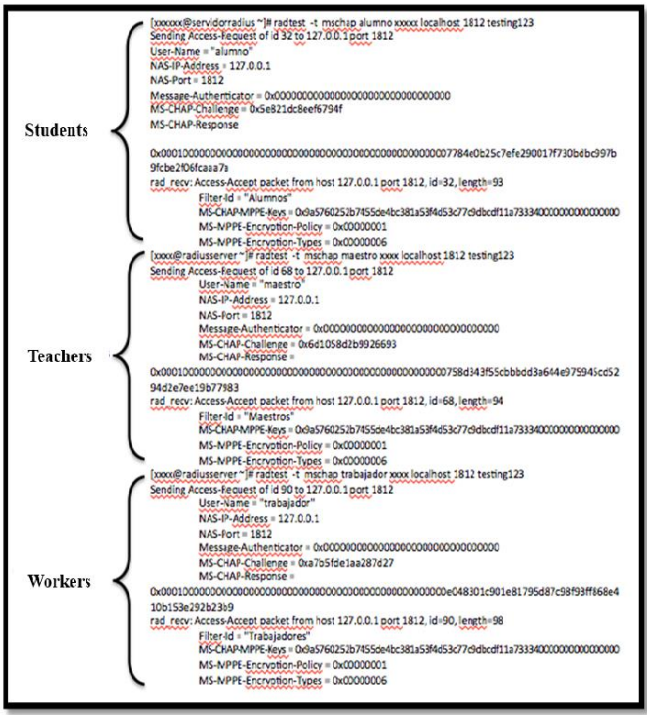

Figure 3. Authentication process for different user profiles (students, teachers, workers).

Security measures involve two-step verification that utilizes FreeRADIUS and MySQL (Inter-institutional Committees for the Evaluation of Higher Education, 2014). The monitoring of the system occurs via NetSight employing SNMPv3.

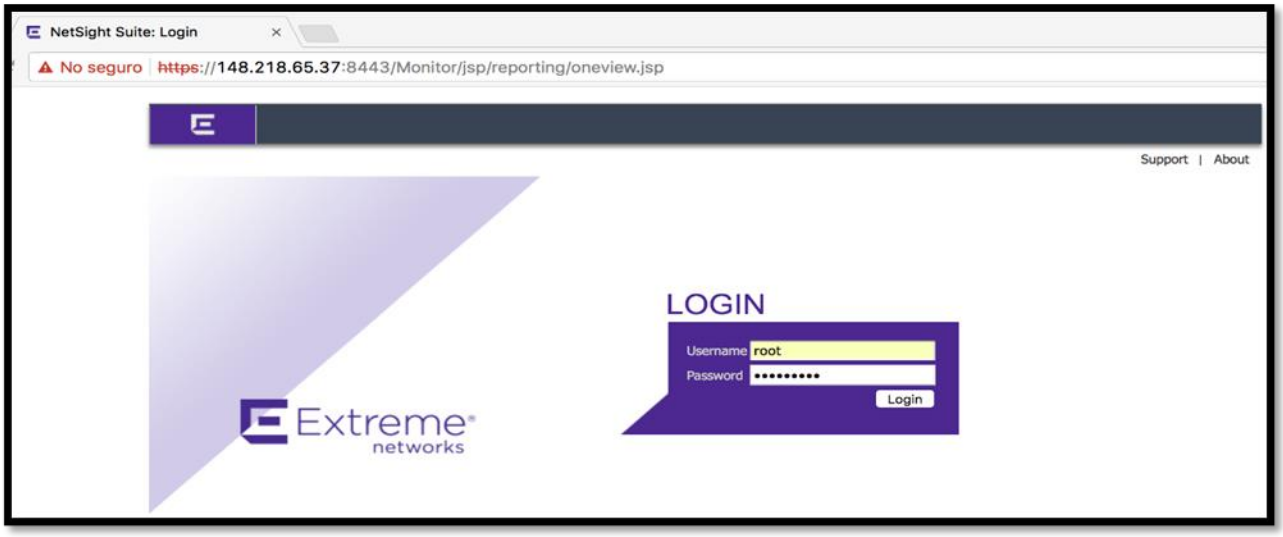

Figure 4. NetSight Suite login interface for monitoring and security management.

In this way, through a unified corporate wireless network solution, with advanced security, control and availability functionalities, it will be possible to meet the requirements and expectations of the UAEM for the benefit of its thousands of users.

5 Results

The deployment in production included 25 buildings, which were equipped with 154 access points to provide reliable service. Internal testing confirmed that security, availability, and coverage needs were met, resulting in a 98% decrease in failures. Wireless coverage was successfully implemented in the targeted areas, and the distribution of access points for each building is specified in the project documents. Furthermore, by using more channels in the 5GHz band, the performance was enhanced, reaching speeds of 150 Mbps.

Table 2. Distribution of Access Points by Building

Buildings	Areas	Aps
Building 1	Module, Fac. Accounting, Building 1 PA, Architecture	18
Building 2	Staff, FCQeI	12
Building 4	Tamulba / Warehouse	2
Building 6	Faculty of Arts/Psychology and Agriculture	4
Building 7	Laboratory Technicians	5
Building 8	Fac. of Psychology, UBM Library	4
Building 9	UBM Computer Center	6
Building 11	UBM Laboratory Technicians	4
Building 12	Maintenance Workshop	1
Building 13	Biomedical Unit	3

Building 14	Cib	4
Building 16	Sitauaem	1
Building 19	Building 19, ICE PB	9
Building 21	Faculty of Law-Computer Center	4
Building 25	Faculty of Law-Library	3
Building 28 - 29	ICE-Computer Center, ICE Administration	8
Building 32	Humanities	4
Building 40	E-uaem, webmsater/mantto, DTC Servers, DTC, Radio, Faculty of Arts-Computer Center	6
Building 41	Ceib	6
Building 44	PB, Mezzanine, Floor 1, Floor 2, Floor 3, Floor 4, Floor 5, Floor 6, Floor 7	19
Building 47	Experimental Field	2
Building 48	CIICAP, CIICAP Grid	14
Building 49	CIQ	10
Building 56	Faculty of Psychology	5
	Total	154

More than 10,000 students and 1000 visitors benefited from access to online academic resources. Load testing validated the solution, with speeds of 50 Mbps downstream and 100 Mbps upstream.

Figure 5. Network speed test results after deployment

In conclusion, thanks to the methodological approach and the technological selection carried out, the objectives set by the university were met in terms of scope of coverage, number of users supported, availability of the service and integration with its authentication, management and monitoring systems.

6 Conclusions

This research effectively established a safe and reliable wireless network for a university. The key accomplishments are:

- Setting up a high-capacity wireless network.
- Creating a method that can be applied to other universities.
- Implementing secure login processes and centralized control.
- Improving safety with two-step verification.

Suggestions for the future involve adding backup plans and refining bandwidth distribution to improve network efficiency

References

Cano, E. V. (2015). Mobile digital devices in education. NARCEA S.A.

Inter-institutional Committees for the Evaluation of Higher Education. (2014, March). www.ciees.edu.mx. Retrieved January 18, 2017, from http://www.ciees.edu.mx/files/Preguntas_frecuentes_de_los_CIEES.pdf

Gartner. (2013, May 1). Technology trends report. Retrieved February 27, 2017, from http://www.gartner.com/newsroom/id/2466615

Information Sciences Institute University of Southern California. (1981, September). RFC 0793 - Transmission Control Protocol (TCP). Retrieved March 10, 2017, from https://www.rfc-es.org/rfc/rfc0793-es.txt

Information Sciences Institute University of Southern California. (1981, September). RFC 791 - Internet Protocol (IP). Retrieved March 10, 2017, from https://tools.ietf.org/html/rfc791

National Institute of Geography and Statistics of Mexico. (2016, May 13). Internet 2016. Retrieved January 28, 2017, from http://www.inegi.org.mx/saladeprensa/aproposito/2016/internet2016_0.pdf

International Organization for Standardization. (1989, February). ISO/IEC 14256. Retrieved March 15, 2017, from https://www.iso.org/standard/14256.html

Pellejero, I. (2006). Fundamentals and applications of security in WLAN networks. Carles Parcerisas.

Network RADIUS SARL. (2016). FreeRADIUS Server Project and Contributors. Retrieved January 8, 2017, from http://freeradius.org/

Ookla. (2017, March 29). Speedtest results. Retrieved from http://www.speedtest.net

González, P. (2015). Pentesting with Kali 2.0. 0xWORD Computing S.L.

van Kleunen, R. (2016). Wireless security in Dubai 2016. Retrieved March 20, 2017, from https://www.bicsi.org/uploadedFiles/BICSI_Website/Global_Community/Presentations/Middle_East_and_Africa/Kleunen_Wireless_Dubai_2016.pdf

Tanenbaum, A. S. (2003). Computer networks (4th ed.). Pearson.