Souphanouvong University Journal of Multidisciplinary Research and Development
2026, Vol. 12, [Fast Track], 211-219
https://doi.org/10.69692/SUJMRD12(Fast track)211

A Development of a Security System and Centralized Authentication for Souphanouvong University's WiFi Network Using Protocol 802.1x and Radius

Sangviane KITTIKHOUN[1], Vinath MEKTHANAVANH[2], Soutthava SIMMAVONG[3], Kalaphath KOUNLAXAY[4], Sayxavath SOUKCHALEUN[5]
[1,2,3,5]*Faculty of Engineering,* [4]*Faculty of Education, Souphanouvong University, Lao PDR.*

[1]*Corresponding author:* Sangviane KITTIKHOUN, *Faculty of Engineering, Souphanouvong University, Lao PDR, E-mail: Sangviane.k@su.edu.la Tel: +8562059595930*

Article Info:
Submitted: May 14, 2026
Revised: May 27, 2026
Accepted: June 2, 2026

Abstract

This research aims to address the inefficiencies in network access control and unequal bandwidth distribution within Souphanouvong University's WiFi network (SUWIFI). The study implemented a centralised authentication and security system using the IEEE 802.1x protocol, a RADIUS server (MikroTik User Manager), and the EAP-TTLS mechanism. The methodology included network topology redesign, centralised database integration, and traffic management using Simple Queues across various user groups. The results demonstrated a significant improvement in network stability and bandwidth allocation. Bandwidth was successfully optimised and limited to 6 Mbps per user, reliably accommodating an average of 150 concurrent users without network congestion. Furthermore, the centralised approach provided robust security against unauthorised access and streamlined administrative tasks. In conclusion, the integration of 802.1x and MikroTik-based RADIUS provides a scalable, secure, and highly efficient network management solution for the university environment.

Keywords: MikroTik, Network Security, RADIUS, VLAN, IEEE 802.1x

1. ພາກສະເໜີ

ໃນຍຸກດິຈິຕອນປັດຈຸບັນ, ເຄືອຂ່າຍອິນເຕີເນັດ ໂດຍສະເພາະເຄືອຂ່າຍບໍ່ມີສາຍ (Wi-Fi) ໄດ້ກາຍເປັນ ພື້ນຖານໂຄງລ່າງທີ່ສຳຄັນສຳລັບການຮຽນ - ການສອນ, ການຄົ້ນຄວ້າ ແລະ ການບໍລິຫານຈັດການພາຍໃນສະຖາ ບັນການສຶກສາ. ມະ ຫາວິທະຍາໄລ ສຸພານຸວົງ ກໍເປັນໜຶ່ງ ໃນສະຖາບັນການສຶກສາຊັ້ນສູງຂອງ ສປປ ລາວ, ເຊິ່ງໄດ້ ເຫັນຄວາມສຳຄັນ ແລະ ນຳເອົາເຕັກໂນໂລຊີ ເປັນຕົ້ນອິນເຕີ ເນັດ (Internet) ເຂົ້າມາໃຊ້ງານເປັນເວລາຫຼາຍປີ (Sinlapaxay et al., 2025). ເຖິງຢ່າງໃດກໍຕາມ, ໃນ ໄລຍະເລີ່ມຕົ້ນ ການນຳໃຊ້ອິນເຕີເນັດຍັງຂາດການວາງ ແຜນທີ່ເປັນລະບົບ ແລະ ການກະຈາຍສັນຍານລະບົບ Network ແມ່ນແບບກະແຈກກະຈາຍ. ເຊິ່ງປະຈຸບັນ ມະຫາວິທະຍາໄລ ສຸພານຸວົງ ປະກອບມີເຄື່ອຄ່າຍທີ່ນຳເຂົ້າ ໃຊ້ຕົວຈິງ 13 ຈຸດ ລວມທັງໝົດ 145 MB ການນຳເຂົ້າ Internet ແມ່ນແຕ່ລະພາກສ່ວນໃຊ້ເຄື່ອຄ່າຍແຕກຕ່າງກັນ, ບໍ່ສາມາດເຊື່ອມໂຍງ ຫຼື Link ຫາກັນໄດ້, ເຊິ່ງສິ່ງຜົນ ກະທົບໃນການກວດສອບການໃຊ້ງານຂອງອິນເຕີເນັດບໍ່ ສາມາດຮູ້ເຖິງປະສິດທິພາບຄວາມໄວຂອງອິນເຕີເນັດໄດ້, ການຄວາມຄຸມຜູ້ໃຊ້ແມ່ນບໍ່ສາມາດຈັດການໄດ້, ການແບ່ງ ຈຳນວນໝາຍເລກໄອພີກໍ່ບໍ່ສາ ມາດບໍລິຫານຈັດການໄດ້, ເມື່ອມີບັນຫາຕ້ອງໄດ້ລົງໄປກວດແກ້ຕາມສະຖານທີ່ນັ້ນໆ ໂດຍກົງເຊິ່ງສ້າງຄວາມບໍ່ສະດວກ, ເສຍຊັບພະຍາກອນ, ເສຍເວລາ, ບໍ່ມາມາດກວດສອບໄດ້ ແລະ ບໍ່ເປັນຈຸດລວມ ສູນ. ເຊິ່ງການເຂົ້າໃຊ້ງານ Internet ແມ່ນຍັງບໍ່ທັນໄດ້ນຳ ໃຊ້ການກວດສອບສິດ (Open Network), ການຄຸ້ມຄອງ ແບນວິດທີ່ບໍ່ມີປະສິດທິພາບ, ແລະ ຍັງບໍ່ທັນມີລະບົບການ ຕິດຕາມຜູ້ໃຊ້ທີ່ບໍ່ຊັດເຈນ ທີ່ສົ່ງຜົນໃຫ້ເກີດບັນຫາໃນການ ຄວບຄຸມການເຂົ້າເຖິງ ແລະ ການຈັດສັນຄວາມໄວອິນເຕີ ເນັດທີ່ບໍ່ເທົ່າທຽມກັນ (Gallardo & Whitacre, 2024). ຈາກການສຳຫຼວດພົບວ່າ ຜູ້ໃຊ້ງານສ່ວນໃຫຍ່ ປະມານ 80% ແມ່ນນັກສຶກສາ ແລະ 20% ແມ່ນຄູ-ອາຈານ ແລະ ພະນັກງານ ເມື່ອມີຄວາມຕ້ອງການໃຊ້ງານເຄືອຂ່າຍພ້ອມໆ ກັນໃນຮູບແບບໂຄງສ້າງພື້ນຖານ (Infrastructure) ຜ່ານ

ຈຸດກະຈາຍສັນຍານ ຫຼື Access Point (AP) (Al-Khraishi & Quwaider, 2020; Pegoraro et al., 2023). ເມື່ອເຄືອຂ່າຍຂະຫຍາຍຕົວ ແລະ ມີຈຳນວນຜູ້ໃຊ້ງານອຸປະກອນ (Node) ເພີ່ມຂຶ້ນ ຈະເຮັດໃຫ້ເກີດບັນຫາຄວາມແອອັດ, ການຍາດແຍ່ງວິດກັນ ແລະ ຄວາມໄວໃນການເຂົ້າເຖິງເຄືອຂ່າຍຈະຫຼຸດລົງຢ່າງຫຼວງຫຼາຍ (Xu et al., 2024) ສະເລ່ຍພຽງ 0.82 Mbps ໃນຊ່ວງເວລາຫຼາຍຄົນໃຊ້ງານ. ນອກຈາກນີ້, ຍັງຂາດກົນໄກການຢືນຢັນຕົວຕົນການເຂົ້າໃຊ້ງານລະບົບ Wi-Fi ເຮັດໃຫ້ບຸກຄົນພາຍນອກທີ່ບໍ່ມີສິດ ສາມາດເຂົ້າເຖິງຂໍ້ມູນຂ່າວສານພາຍໃນໄດ້ງ່າຍ, ສ່ຽງຕໍ່ການຖືກໂຈມຕີທາງໄຊເບີ, ການລັກລອບເອົາຂໍ້ມູນສຳຄັນ ແລະ ອື່ນໆ. ບັນຫາດັ່ງກ່າວ ສົ່ງຜົນກະທົບໂດຍກົງຕໍ່ປະສິດທິພາບການໃຊ້ງານ, ການຮຽນ-ການສອນ ແລະ ການຄົ້ນຄວ້າ ເຊິ່ງຕ້ອງອາໄສອິນເຕີເນັດຄວາມໄວສູງ ແລະ ມີຄວາມໝັ້ນຄົງ. ດັ່ງນັ້ນ, ຈຶ່ງມີຄວາມຈຳເປັນອັນຮີບດ່ວນທີ່ຕ້ອງປັບປຸງລະບົບການບໍລິຫານເຄືອຂ່າຍໃຫ້ທັນສະໄໝ, ປອດໄພ, ຄອບຄຸມການເຂົ້າເຖິງ ແລະ ຈັດສັນແບນວິດໃຫ້ເທົ່າທຽມກັນ. ການຄົ້ນຄວ້າຄັ້ງນີ້ຈຶ່ງມີຄວາມສຳຄັນເພື່ອແກ້ໄຂບັນຫາການຂາດການຄອບຄຸມ ແລະ ຄວາມບໍ່ປອດໄພ ໂດຍການອອກແບບ ແລະ ພັດທະນາລະບົບເຄືອຂ່າຍບໍ່ມີສາຍທີ່ນຳໃຊ້ລະບົບຢືນຢັນຕົວຕົນແບບລວມສູນຜ່ານ RADIUS (Hoffmann et al., 2025) ຮ່ວມກັບມາດຕະຖານ IEEE 802.1x (Akshay et al., 2025) ເພື່ອບໍລິຫານຈັດການລະບົບເຄືອຂ່າຍແບບບໍ່ມີສາຍ ແລະ ແບບມີສາຍຢ່າງປອດໄພ (Al-Absi et al., 2021; Christanto et al., 2025), ຄຽງຄູ່ກັບການເພີ່ມປະສິດທິພາບແບນວິດດ້ວຍ Simple Queues ເພື່ອຊ່ວຍໃຫ້ຜູ້ບໍລິຫານລະບົບສາມາດຄອບຄຸມ ແລະ ຈັດການແບນວິດໄດ້ຢ່າງມີປະສິດທິພາບ (Januantoro, 2025) & (Novianto et al., 2021), ສ້າງຄວາມສາມາດຂະຫຍາຍຂອງລະບົບ Network ຜ່ານ VLAN ແລະ ເພື່ອເປັນຕົວແບບໃຫ້ສະຖາບັນອື່ນໆ.

2. ອຸປະກອນ ແລະ ວິທີການ

ໃນການຄົ້ນຄວ້າທົດລອງໃນຄັ້ງນີ້ໄດ້ນຳໃຊ້ອຸປະກອນຮາດແວ (Hardware) Mikrotik, Switch Cisco Wireless Access Point, Smart Phone, Laptop, Tablet ແລະ ຊອບແວ (Software) ເພື່ອນຳໃຊ້ເຂົ້າໃນການຕິດຕັ້ງ ແລະ ກວດສອບການໃຊ້ງານ.

2.1 ເຄື່ອງມືໃນການຄົ້ນຄວ້າ

ເຄື່ອງມືຫຼັກທີ່ນຳເຂົ້າມາໃນການທົດລອງຄົ້ນຄວ້າວິໄຈໃນຄັ້ງນີ້ປະກອບດ້ວຍອຸປະກອນຮາດແວ (Hardware) ແລະ ຊອບແວ (Software) ເຂົ້າໃນການຄົ້ນຄວ້າ (ຕາຕະລາງທີ 1 ແລະ ຕາຕະລາງທີ 2)

2.2 ວິທີການທົດລອງ

ຕົວຢ່າງການທົດລອງສຳລັບການວິໄຈໃນຄັ້ງນີ້ ແມ່ນໄດ້ນຳເອົາຄູ, ອາຈານ - ພະນັກງານ ແລະ ນັກສຶກສາທີ່ໄດ້ມີການຈັດການຮຽນ-ການສອນ, ຜູ້ເຂົ້າໃຊ້ບໍລິການອິນເຕີເນັດຂອງສູນຂໍ້ມູນ ແລະ ຂ່າວສານຂອງມະຫາວິທະຍາໄລ ສຸພານຸວົງ ຈຳນວນທັງໝົດ 1000 ຄົນ ເຂົ້າໃນການລົງທະບຽນ, ທົດລອງການໃຊ້ງານລະບົບ, ການກະຈາຍສັນຍານຂອງລະບົບເພື່ອທົດສອບຄວາມໄວຂອງການໃຊ້ງານຂອງການຮັບ - ສົ່ງຂໍ້ມູນ ແລະ ຄົ້ນຫາຈຸດບົກຜ່ອງເພື່ອແກ້ໄຂປັບປຸງລະບົບ WiFi ໃຫ້ມີຄວາມສະຖຽນ, ມີການຕິດຕາມກວດກາການເຂົ້າໃຊ້ງານ ໃຫ້ມີຄວາມປອດໄພມີມາດຕະຖານລະດັບສາກົນດ້ວຍການນຳໃຊ້ເຕັກໂນໂລຊີດ້ານການກະຈາຍສັນຍານເຂົ້າມາຊ່ວຍໃນລະບົບ (ຮູບພາບທີ 1).

2.2.1 ແຜນຜັງໂຄງສ້າງລະບົບ (Network Topology)

ຈາກການອອກແບບລະບົບທົດລອງ ໂຄງສ້າງທາງກາຍະພາບ (Physical Topology) ທັງກ່ອນ ແລະ ຫຼັງການປັບປຸງແມ່ນມີລັກສະນະຄືກັນ ໂດຍສັນຍານອິນເຕີເນັດຈະເຊື່ອມຕໍ່ເຂົ້າຫາ MikroTik Router ທີ່ເປັນ Gateway ຫຼັກ ແລ້ວສົ່ງຕໍ່ສາຍໄປຫາ Cisco Switch ເພື່ອກະຈາຍສັນຍານໄປຫາ Access Point ແຕ່ລະຈຸດ (SU1-SU9) ແຕ່ໄດ້ມີຄວາມແຕກຕ່າງກັນຢ່າງຊັດເຈນໃນການຕັ້ງຄ່າທາງຕັກກະສາດ (Logical Configuration) ທີ່ປັບປຸງໃໝ່ ໂດຍມີການນຳໃຊ້ລະບົບ Network Security (IEEE 802.1X) ແລະ RADIUS Server ເຂົ້າມາບໍລິຫານຈັດການ ເຮັດໃຫ້ເມື່ອມີອຸປະກອນ Client ພະຍາຍາມເຊື່ອມຕໍ່ Wi-Fi ອຸປະກອນ AP ໄດ້ສົ່ງຂໍ້ມູນໄປກວດສອບສິດ (Authentication) ກັບ RADIUS Server ເຊັ່ນ: FreeRADIUS, Windows Server NPS ຫຼື MikroTik User Manager ທີ່ຜູກໄວ້ໃນລະບົບກ່ອນ ຈຶ່ງໄດ້ຮັບອະນຸຍາດໃຫ້ເຂົ້າໃຊ້ງານເຄືອຂ່າຍໄດ້(ຮູບພາບທີ 2).

2.2.2 ເຊີເວີການພິສູດຢືນຢັນຕົວຕົນ (Authentication Server)

ສຳລັບສ່ວນເຄື່ອງແມ່ຂ່າຍ ໄດ້ມີການທົດລອງຕິດຕັ້ງລະບົບປະຕິບັດການ Debian ພ້ອມແອັບພລິເຄຊັນ FreeRADIUS ແລະ ຖານຂໍ້ມູນ OpenLDAP ເທິງເຊີ

ເວີທີ່ມີຄຸນສົມບັດຮາດແວຄື CPU 3.5 GHz, RAM 2 GB ແລະ HDD 100 GB ຮ່ວມກັບການນຳໃຊ້ MikroTik User Manager ເພື່ອເປັນ RADIUS ສຳລັບການຈັດການຜູ້ໃຊ້ແບບລວມສູນ ໂດຍເຮັດໜ້າທີ່ພິສູດຕົວຕົນ (Authentication) ວ່າຊື່ຜູ້ໃຊ້ແລະລະຫັດຜ່ານຖືກຕ້ອງຫຼືບໍ່, ອະນຸຍາດສິດ (Authorization) ໃນການກຳນົດສິດເຂົ້າເຖິງເຄືອຂ່າຍ ເຊັ່ນ: ການສົ່ງຄ່າຂອງແຕ່ລະ VLAN ກັບຄືນໄປຫາ Switch/AP, ແລະ ບັນທຶກຂໍ້ມູນ (Accounting) ປະຫວັດການໃຊ້ງານ ເຊັ່ນ ບຸກຄົນ ເວລາເຂົ້າແລະອອກລະບົບ ເພື່ອໃຊ້ໃນການກວດສອບຄວາມປອດໄພຍ້ອນຫຼັງ.

2.2.3 ການການິດຖານຂໍ້ມູນ ແລະ ກຸ່ມຜູ້ໃຊ້

ເຄືອຂ່າຍ SUWIFI ໄດ້ສ້າງໄດເຣັກທໍຣີ (Directory) ໂດຍໃຊ້ OpenLDAP ແລະ Hotspot Database ເພື່ອເກັບກຳຂໍ້ມູນຜູ້ໃຊ້ງານ. ໂຄງສ້າງການຈັດການໄດ້ແບ່ງອອກເປັນ: ກຸ່ມນັກສຶກສາ, ຄູອາຈານ ແລະ ແຂກ (ດັ່ງຮູບພາບທີ 3).

ເມື່ອຕິດຕັ້ງບໍລິການ Hotspot ແລ້ວ, ຈຳເປັນຕ້ອງເພີ່ມຂໍ້ມູນສະເພາະໃສ່ໄຟລ໌ຫຼັກຂອງລະບົບໂດຍການໃຊ້ຄຳສັ່ງ dpkg-reconfigure slapd. ຂໍ້ມູນທີ່ຕື່ມໃສ່ໃນໄຟລ໌ແມ່ນ:

- Organization name: WIFISU, RADIUS
- Password: ****
- Database engine: MDB

2.2.4 ການຈັດການຜູ້ໃຊ້ດ້ວຍ Access Point ແລະ User Manager

ມີຈຸດກະຈາຍສັນຍານ (APs) ຈຳນວນ 4 ຈຸດ ທີ່ມີຢູ່ໃນເຄືອຂ່າຍໄຮ້ສາຍ ເຊິ່ງທຸກຈຸດກະຈາຍ SSID ດຽວກັນ. ຈຸດເຫຼົ່ານີ້ຖືກຄວບຄຸມລວມສູນໂດຍ MikroTik ຜ່ານລະບົບ CAPsMAN ພາຍໃຕ້ວົງເຄືອຂ່າຍ (VLAN) ດຽວກັນ ເພື່ອອະນຸຍາດໃຫ້ຜູ້ໃຊ້ສາມາດໂຣມມິ່ງ (Roaming) ໄດ້. ອີງຕາມການສຳຫຼວດພົບວ່າ ຜູ້ໃຊ້ 80% ແມ່ນນັກສຶກສາ ແລະ 20% ແມ່ນພະນັກງານ-ຄູອາຈານ. ເພື່ອປ້ອງກັນການດຶງແບນວິດກັນ, ລະບົບໄດ້ໃຊ້ໂໝດ Simple Queues ຜ່ານ User Manager ໂດຍກຳນົດ Profile ແລະ ຈຳກັດອັດຕາການຮັບ-ສົ່ງຂໍ້ມູນໃຫ້ທຸກກຸ່ມມີສິດເທົ່າທຽມກັນ (ຮູບພາບທີ 4).

3. ຜົນໄດ້ຮັບ

3.1 ການຄວບຄຸມອັດຕາການຮັບ-ສົ່ງຂໍ້ມູນ (Bandwidth Management)

ໃນໄລຍະທຳອິດກ່ອນການປັບປຸງ, ການໃຊ້ຊັບພະຍາກອນບໍ່ມີປະສິດທິພາບ ເນື່ອງຈາກບໍ່ມີການຄວບຄຸມການ ແຈກຢາຍຂໍ້ມູນ. ຜູ້ໃຊ້ບາງຄົນໃຊ້ແບນວິດຫຼາຍເກີນໄປ ເຮັດໃຫ້ຄວາມໄວອິນເຕີເນັດລວມຊ້າລົງ (ດາວໂຫຼດສະເລ່ຍພຽງ 0.82 Mbps, (ຮູບພາບທີ 5). ຫຼັງຈາກນຳໃຊ້ວິທີການ Simple Queues ໃນເຣົາເຕີ MikroTik ຮ່ວມກັບລະບົບຢືນຢັນຕົວຕົນ ໄດ້ຮັບຜົນທີ່ດີຄື:

- ອັດຕາຄວາມໄວຖືກກຳນົດໃຫ້ຜູ້ໃຊ້ແຕ່ລະບັນຊີຢູ່ທີ່ 6 Mbps ຢ່າງຄົງທີ່ (ແທນທີ່ຈະປ່ອຍອິດສະຫຼະເຖິງ 10 Mbps ແຕ່ບໍ່ສະຖຽນ).
- ປະຈຸບັນ ລະບົບສາມາດຮອງຮັບຜູ້ໃຊ້ສະເລ່ຍ 150 ຄົນໃນເວລາພ້ອມກັນ ໂດຍທີ່ທຸກຄົນໄດ້ຮັບແບນວິດພຽງພໍສຳລັບການນຳໃຊ້ ແລະ ບໍ່ເຮັດໃຫ້ເຄືອຂ່າຍລົ້ມເຫຼວ.
- ປະສິດທິພາບໃນການທົດສອບຄວາມໄວ (Speed test) ສະແດງໃຫ້ເຫັນການຈັດສັນທີ່ດີຂຶ້ນຢ່າງຊັດ (ຮູບພາບທີ 6).

3.2 ການຕິດຕາມຜູ້ໃຊ້ງານໃນລະບົບ (Networking Monitoring)

ນອກຈາກການຄວບຄຸມແບນວິດແລ້ວ, ລະບົບຍັງສາມາດຕິດຕາມການນຳໃຊ້ຂໍ້ມູນຂອງຜູ້ໃຊ້ແຕ່ລະຄົນໃນແຕ່ລະ VLAN ໄດ້ຢ່າງຊັດເຈນ. ຜົນການທົດສອບ (ຮູບພາບທີ 7 ແລະ 8) ສະແດງໃຫ້ເຫັນວ່າຜູ້ໃຊ້ທີ່ຖືກຈັດສັນໃນ VLAN ທີ່ແຕກຕ່າງກັນ (ເຊັ່ນ: VLAN 20; 60; 70; 90) ຖືກຄວບຄຸມຢ່າງເປັນລະບຽບ ໂດຍຜູ້ດູແລລະບົບສາມາດກວດສອບສະ ຖານະການເຮັດວຽກ (Uptime) ແລະ ອັດຕາການດາວໂຫຼດ/ອັບໂຫຼດ (Rx Rate/Tx Rate) ໄດ້ແບບສົດໆ (Real-time) (ຮູບພາບທີ 7) (ຮູບພາບທີ 8).

4. ວິພາກ

ການບັງຄັບລົງທະບຽນຜູ້ໃຊ້ໃນລະບົບ Hotspot SUWIFI ທີ່ປະສົມປະສານກັບໂປຣໂຕຄອນ 802.1x ໄດ້ຊ່ວຍຍົກລະດັບຄວາມປອດໄພຂອງເຄືອຂ່າຍຢ່າງຫຼວງຫຼາຍ ຜູ້ໃຊ້ທຸກຄົນຕ້ອງມີຊື່ບັນຊີ (Username) ແລະ ລະຫັດຜ່ານ (Password) ສະເພາະຕົວ, ເຊິ່ງເປັນການປ້ອງກັນການເຂົ້າເຖິງຈາກບຸກຄົນພາຍນອກທີ່ບໍ່ໄດ້ຮັບອະນຸຍາດ. ຂໍ້ໄດ້ປຽບຫຼັກຂອງ 802.1x ຄື: ມີຄວາມປອດໄພສູງ, ຈັດການບັນຊີງ່າຍ, ປະຢັດແບນວິດ ແລະ ຫຼຸດພາລະການປະມວນຜົນຂອງຮາດແວທີ່ບໍ່ຈຳເປັນ. ງານວິໄຈຂອງພວກ

ເຮົາມີຄວາມໂດດເດັ່ນກວ່າ ໃນດ້ານການສ້າງລະບົບທີ່ເຮັດວຽກຮ່ວມກັບ MikroTik User Manager ເຊິ່ງຊ່ວຍເພີ່ມຄວາມສາມາດໃນການກຳນົດຄ່າ Session, ຄວາມໄວ ແລະ ຕິດຕາມການນຳໃຊ້ອິນເຕີເນັດການວິໄຈຄັ້ງນີ້ໄດ້ຮັບຜົນທີ່ໜ້າພໍໃຈ ເມື່ອສົມທຽບກັບບົດຄົ້ນຄວ້າຂອງ Riyantana et al. (2024) ທີ່ສ້າງເຄືອຂ່າຍໃນຮູບແບບ VLAN ເຊິ່ງມີຄວາມປອດໄພ ແຕ່ຍັງມີຂໍ້ຈຳກັດໃນການບໍລິຫານຈັດການຜູ້ໃຊ້.

ລະບົບລວມສູນນີ້ ຊ່ວຍໃຫ້ການກວດສອບການເຮັດວຽກຂອງເຄືອຂ່າຍມີຄວາມທົ່ວເຖິງ ແລະ ວ່ອງໄວກວ່າໂຄງສ້າງລະບົບເກົ່າ ເຫັນວ່າລະບົບຂອງພວກເຮົາເປັນການຍົກລະດັບມາດຕະຖານຄວາມປອດໄພ ແລະ ການບໍລິຫານຈັດການໃຫ້ເປັນລະດັບ Enterprise ໂດຍການນຳໃຊ້ໂປຣໂຕຄອນ 802.1x ແລະ EAP-TTLS ເພື່ອປ້ອງກັນການເຂົ້າເຖິງຈາກບຸກຄົນພາຍນອກ, ເຊິ່ງມີຄວາມປອດໄພສູງກວ່າລະບົບ Hotspot ທົ່ວໄປຢ່າງຊັດເຈນ, ດ້ານປະສິດທິພາບ, ລະບົບມີການຈັດການ Bandwidth ທີ່ດີເລີດ ໂດຍການກຳນົດຄວາມໄວໃຫ້ຜູ້ໃຊ້ແຕ່ລະຄົນຢ່າງເໝາະສົມ ເພື່ອແກ້ໄຂບັນຫາການຍາດແຍ່ງອິດ ແລະ ຮັກສາຄວາມສະຖຽນ (Stability) ເຖິງວ່າຈະມີການໃຊ້ງານໜາແໜ້ນ. ນອກຈາກນັ້ນ, ຍັງຮອງຮັບການຂະຫຍາຍຕົວ (Scalability) ໃນພື້ນທີ່ກວ້າງດ້ວຍລະບົບ CAPsMAN ແລະ VLAN ທີ່ຊ່ວຍໃຫ້ການຈັດການ Access Point ເປັນແບບລວມສູນ ແລະ ສາມາດໃຊ້ງານ Roaming (ຍ້າຍຈຸດເຊື່ອມຕໍ່ໄດ້ໂດຍເນັດບໍ່ຫຼຸດ). ທັງໝົດນີ້ຖືກຄວບຄຸມຜ່ານ RADIUS Server ທີ່ເຊື່ອມຕໍ່ກັບ OpenLDAP, ເຊິ່ງເປັນມາດຕະຖານການຈັດການຖານຂໍ້ມູນຜູ້ໃຊ້ໃນລະດັບສາກົນ ຖ້າທຽບໃສ່ການສຶກສາຂອງ Hazairin (2024) ທີ່ມີການຕັ້ງຄ່າອິນເຕີເຟດເຣົາເຕີ Mikrotik, ການຕັ້ງຄ່າ DHCP Client, ການຕັ້ງຄ່າທີ່ຢູ່ IP ຂອງເຄືອຂ່າຍຮ້ອດສະປອດ, ການຕັ້ງຄ່າໄຟວໍ NAT ແຕ່ເຫັນວ່າການສຶກສາຂອງພວກເຮົາທີ່ໄດ້ໃຊ້ RADIUS Server ທີ່ເຊື່ອມຕໍ່ກັບ Open LDAP ໃນການບໍລິຫານ Hotspot ການນຳໃຊ້ RADIUS Server (Remote Authentication Dial-In User Service) ແມ່ນການຍົກລະດັບການຈັດການເຄືອຂ່າຍຈາກແບບທົ່ວໄປຂຶ້ນມາເປັນລະດັບ Enterprise (ອີງກອນມາດຕະຖານ). ທີ່ເຮັດໜ້າທີ່ເປັນ "ສູນກາງການກວດສອບສິດ" (ຕາຕະລາງທີ 3).

5. ສະຫຼຸບ

ຜົນໄດ້ຮັບຂອງບົດວິໄຈ “ພັດທະນາລະບົບຮັກສາຄວາມປອດໄພ ແລະ ການຢືນຢັນຕົວຕົນແບບລວມສູນສຳລັບເຄືອຂ່າຍ Wi-Fi ມະຫາວິທະຍາໄລສຸພານຸວົງ ໂດຍນຳໃຊ້ 802.1X ແລະ RADIUS” ສາມາດສະຫຼຸບໄດ້ດັ່ງນີ້:

- ລະບົບໃໝ່ສາມາດເພີ່ມຄວາມປອດໄພໃນເຄືອຂ່າຍ Wi-Fi ໄດ້ຢ່າງມີປະສິດທິພາບ ໂດຍນຳໃຊ້ IEEE 802.1X, RADIUS ແລະ EAP-TTLS ເພື່ອກວດສອບສິດຜູ້ໃຊ້ ກ່ອນເຂົ້າໃຊ້ງານ
- ການຈັດການແບນວິດມີປະສິດທິພາບຂຶ້ນ ໂດຍນຳໃຊ້ Simple Queues ໃນ MikroTik ເພື່ອແບ່ງຄວາມໄວໃຫ້ຜູ້ໃຊ້ແຕ່ລະຄົນຢ່າງເທົ່າທຽມ ລະບົບກຳນົດຄວາມໄວໄວ້ທີ່ 6 Mbps ຕໍ່ຄົນ
- ກ່ອນໜ້າມີຄວາມໄວ Internet ສະເລ່ຍພຽງ 0.82 Mbps ໃນເວລາທີ່ມີຜູ້ໃຊ້ຫຼາຍ ແຕ່ຫຼັງປັບປຸງ ລະບົບສາມາດຄວບຄຸມຄວາມໄວໄດ້ດີ ທີ່ 0.94 Mbps ແລະ ລົດບັນຫາການດຶງແບນວິດກັນ
- ລະບົບສາມາດຮອງຮັບຜູ້ໃຊ້ພ້ອມກັນໄດ້ປະມານ 150 ຄົນ ໂດຍບໍ່ເກີດບັນຫາເຄືອຂ່າຍຫຼົ້ມ
- ລະບົບສາມາດຕິດຕາມຜູ້ໃຊ້ໃນແຕ່ລະ VLAN ໄດ້ຊັດເຈນ ເຮັດໃຫ້ການກວດສອບ ແລະ ບໍລິຫານເຄືອຂ່າຍງ່າຍຂຶ້ນ
- ການບໍລິຫານແບບລວມສູນຊ່ວຍຫຼຸດຂັ້ນຕອນການຈັດການຂອງເບິ່ງແຍງແລລະບົບ ແລະ ສາມາດຂະຫຍາຍລະບົບໄດ້ໃນອະນາຄົດ
- ໂດຍລວມ ຜົນການຄົ້ນຄວ້າພິສູດວ່າ: ການນຳໃຊ້ MikroTik ຮ່ວມກັບ IEEE 802.1X, RADIUS ແລະ VLAN ສາມາດສ້າງລະບົບ Wi-Fi ທີ່ມີຄວາມປອດໄພ, ສະຖຽນ ແລະ ມີປະສິດທິພາບ ເໝາະສຳລັບສະຖາບັນການສຶກສາ ແລະ ສະຖານທີ່ອື່ນໄດ້.

6. ຂໍ້ຂັດແຍ່ງ

ຂ້າພະເຈົ້າໃນນາມຜູ້ຄົ້ນຄວ້າວິທະຍາສາດ ຂໍປະຕິຍານຕົນ ວ່າ ຂໍ້ມູນທັງໝົດທີ່ມີໃນບົດຄວາມວິຊາການດັ່ງກ່າວນີ້ ແມ່ນບໍ່ມີຂໍ້ຂັດແຍ່ງທາງຜົນປະໂຫຍດກັບພາກສ່ວນໃດ ແລະ ບໍ່ໄດ້ເອື້ອປະໂຫຍດໃຫ້ກັບພາກສ່ວນໃດພາກສ່ວນໜຶ່ງ, ກໍລະນີມີການລະເມີດໃນຮູບການໃດຮູບການໜຶ່ງ ຂ້າພະເຈົ້າມີຄວາມຍິນດີ ທີ່ຈະຮັບຜິດຊອບແຕ່ພຽງຜູ້ດຽວ.

7. ເອກະສານອ້າງອີງ

Akshay, C., Jacob, A. S., Nandini, G. K., & Nath, H. V. (2025). IEEE 802.1X

Authentication and Security Mechanisms in Modern Networks. 2025 4th International Conference on Advances in Computing, Communication, Embedded and Secure Systems (ACCESS),

Al-Absi, M. A., Al-Absi, A. A., Sain, M., & Lee, H. (2021). Moving ad hoc networks—a comparative study. *Sustainability*, *13*(11), 6187. https://doi.org/https://doi.org/10.3390/su13116187

Al-Khraishi, T., & Quwaider, M. (2020). Performance evaluation and enhancement of VLAN via wireless networks using OPNET modeler. *arXiv preprint arXiv:2007.06997*, *12*. https://doi.org/https://doi.org/10.5121/ijwmn.2020.12302

Atsuya, Y., Ayed, S. B., & Teraoka, F. (2011). Network access authentication infrastructure using EAP-TTLS on diameter EAP application. Proceedings of the 7th Asian Internet Engineering Conference,

Christanto, F. W., Cholillah, P., & Hirzan, A. M. (2025). Optimizing Mikrotik-Based Network Security using Address List, Firewall Filter Rules, and Raw Firewall. *Revista de Informática Teórica e Aplicada*, *32*(3), 66-76. https://doi.org/https://doi.org/10.22456/2175-2745.142954

Gallardo, R., & Whitacre, B. (2024). An unexpected digital divide? A look at internet speeds and socioeconomic groups. *Telecommunications Policy*, *48*(6), 102777.

Hazairin, F., Tumardiana, Ye. (2024). DESIGNING A WEB-BASED MIKROTIK HOTSPOT SERVER MONITORING APPLICATION. *JURNAL KOMPUTER, INFORMASI DAN TEKNOLOGI (JKOMITEK) Учредители: Penerbit ADM Bengkulu*, *4*(1), 11. https://doi.org/10.53697/jkomitek.v4i1.1745

Hoffmann, E. F., Machado, C., & Westphall, C. M. (2025). RadChain Connect: Integration Between Blockchain and FreeRADIUS for Secure Authentication in Wi-Fi Networks/Web Environment. 2025 International Conference on Information Networking (ICOIN),

Januantoro, A. (2025). Network Security Strengthening Strategy Using Mikrotik Firewall on Small to Medium-Scale IT Infrastructure. International Conference of Innovation and Community Engagement,

Martínez, V. M., Ribeiro, M. R., & Mota, V. F. (2024). Wi-Fi faces the new wireless ecosystem: a critical review. *Annals of telecommunications*, *79*(5), 397-413.

Mustain, M., Munif, M., Mauladi, K. F., & Susilo, P. H. (2025). Integrasi Radius Server Dengan Database Mysql Untuk Login Hotspot Mikrotik Pada Lingkungan Kampus. *JUSIBI (Jurnal Sistem Informasi dan E-Bisnis)*, *7*(2), 52-62. https://doi.org/https://doi.org/10.54650/jusibi.v7i2.600

Novianto, D., Tommy, L., & Japriadi, Y. S. (2021). Implementation of a Network Security System Using the Simple Port Knocking Method on a Mikrotik-Based Router Implementasi Sistem Keamanan Jaringan Menggunakan Metode Simple Port Knocking Pada Router Berbasis Mikrotik. *JURNAL KOMITEK*, *1*(2), 407-417.

Pegoraro, J., Lacruz, J. O., Meneghello, F., Bashirov, E., Rossi, M., & Widmer, J. (2023). RAPID: Retrofitting IEEE 802.11 ay access points for indoor human detection and sensing. *IEEE Transactions on Mobile Computing*, *23*(5), 4501-4519. https://doi.org/10.1109/TMC.2023.3291882

Riyantana, I., Pertama, P., & Sudarsana, I. M. (2024). Optimalisasi Jaringan Internet Berbasis Mikrotik dengan Metode VLAN di Kelurahan Kapal Mengwi Badung. *Semin. Has. Penelit. Inform. dan Komput.(SPINTER)| Inst. Teknol. dan Bisnis STIKOM Bali*, *1*(2), 224-229.

Sinlapaxay, S., Amphai, V., Bounhome, M., Bounthanome, V., & Phoneouthai, T. (2025). Performance Comparison of Internet Service from Best Telecom ETL Unitel and Laotelecom at Souphanouvong University. *Souphanouvong University Journal Multidisciplinary Research and Development*, *11*(2), 49-56. https://doi.org/https://doi.org/10.69692/SUJMRD110249

Xu, M., Chen, B., Tan, Z., Chen, S., Wang, L., Liu, Y., San, T. I., Fong, S. W., Wang, W., & Feng, J. (2024). AHAC: advanced network-hiding access control framework. *Applied Sciences*, *14*(13), 5593.

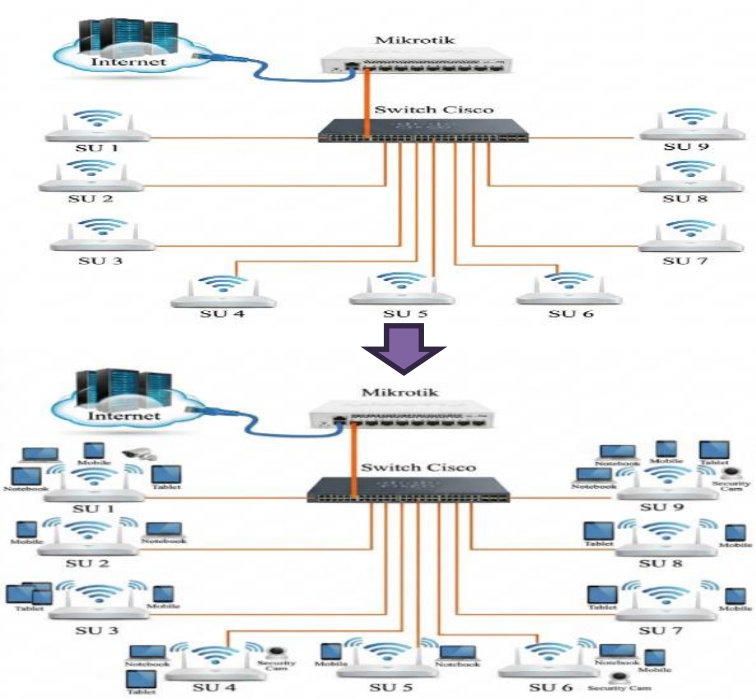
ตาตาลางที 1. ธาดแอ (Hardware)

ลายการ	ปะเพด/ยี่ห้	ฟ้าที่
MikroTik	CCR1009-7G-1C-1S+	ถอบถุม Router และ ละบับเถือข่าย
Switch Cisco	Catalyst 2960 Plus Series	เชื่อมต่อุปะกอบในเถือข่าย LAN
Wireless Access Point	tp-link	ถือกะจายสันยาน Wi-Fi
สาย Lan	Cat 5	เชื่อมต่อุปะกอบ Network หื Internet
Smart Phone, Laptop, Tablet.	Android/iOS, Windows/macOS	เชื่อมต่ Wi-Fi
Console Line		Config.

ตาตาลางที 2. ซอบแอ (Software)

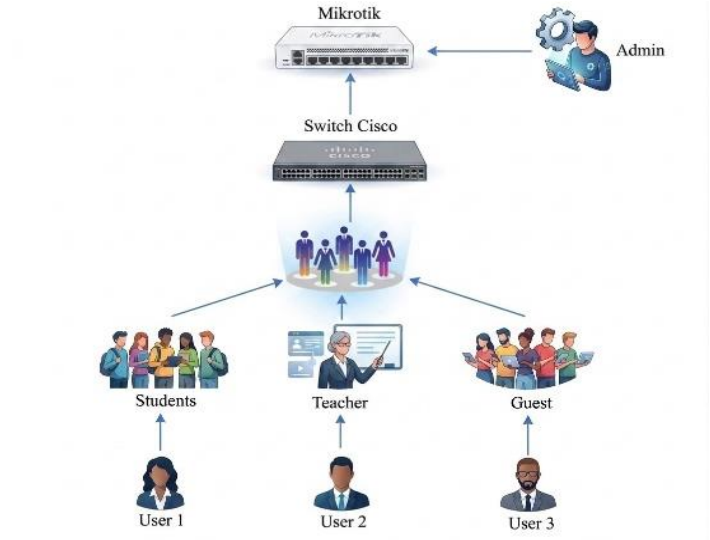
ลายการ	เอิชัน	ฟ้าที่
MikroTik RouterOS	6.49.10	ธองธับฟังชัน RADIUS Client, ละบับ Hotspot/User Manager
WinBox	3.40	Configure ตั้งถ่า
Web Browser	Chrome/Firefox	ใช้งาน, บลิหานจัดการ
Putty	0.83	ใช้เฮ้าในการ Config

รูบพาบที 1: ขั้นตอนการถิ้นถอ้าอิใจ



ຮູບພາບທີ 2: ໂທໂພໂລຢີກ່ອນ ແລະ ຫຼັງການຈັດຕັ້ງປະຕິບັດ

suwifi, radius

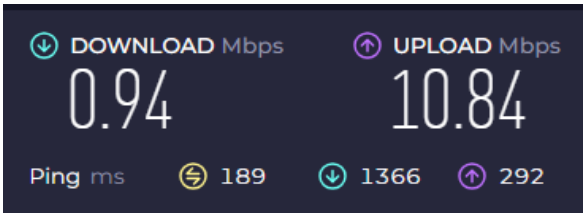


ຮູບພາບທີ 3: ກຸ່ມຜູ້ໃຊ້

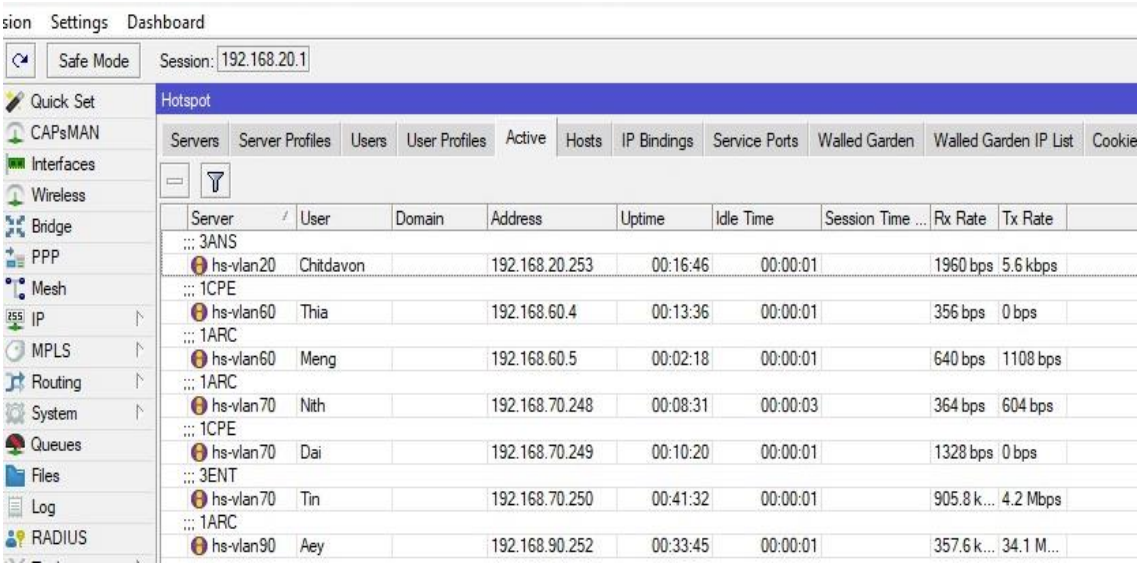
Server	Name	Address	MAC ...	Profil
all	Anjy			FET
:: 2GBM				
all	Kiengkham			FET
:: 2GBM				
all	Konuji			FET
:: 2GBM				
all	Vanhphen			FET
:: 2GBM				

ຮູບພາບທີ 4: ທົດສອບຄວາມຖືກຕ້ອງຂອງຜູ້ໃຊ້.

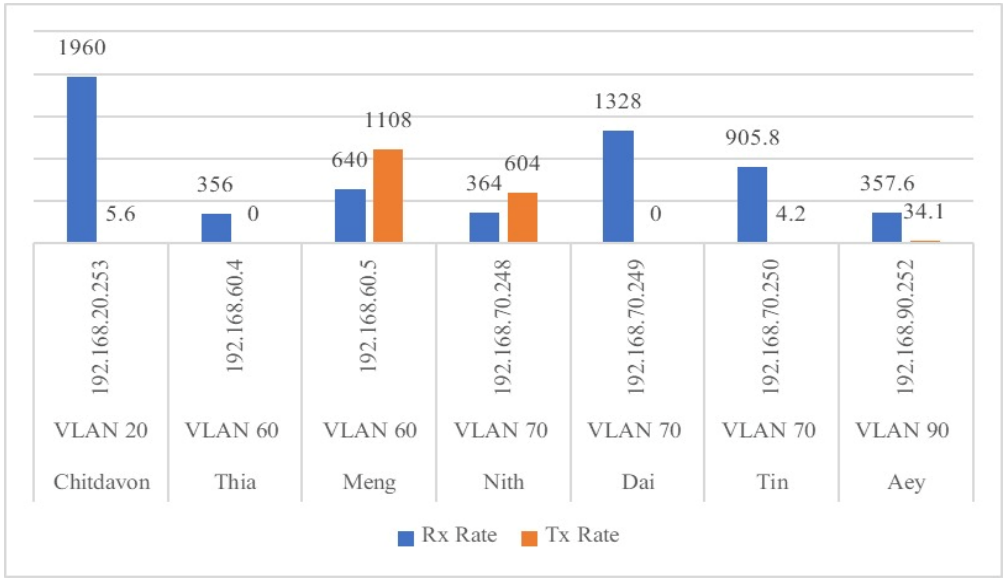
ຮູບພາບທີ 5: ຄວາມໄວຂອງອິນເຕີເນັດກ່ອນການຈັດຕັ້ງປະຕິບັດ



ຮູບພາບທີ 6: ຄວາມໄວຂອງອິນເຕີເນັດຫຼັງການຈັດຕັ້ງປະຕິບັດ



ຮູບພາບທີ 7: ກວດສອບຜູ້ໃຊ້ອິນເຕີເນັດໃນລະບົບ



ຮູບພາບທີ 8: ກວດສອບຜູ້ໃຊ້ອິນເຕີເນັດໃນລະບົບ

ຕາຕະລາງ 3. ຄວາມແຕກຕ່າງລະຫວ່າງ Vlan ແລະ Hotspot ໃນ Mikrotik.

Feature	VLAN (Virtual LAN)	Hotspot
Layer	Layer 2 (Data Link)	Layer 3-4 (Network/Transport)
Primary Purpose	Network Isolation & Segmentation	User Authentication & Billing
Method	Tags Ethernet frames (802.1Q)	Captive Portal (Web login)
Scalability	High (Used for large, complex networks)	Best for guest networks (Hotels, Cafes, University)
Hardware Requirement	Needs VLAN-aware switches/APs	Works on any interface (Wireless, Ethernet)