

การจัดการบัญชีผู้ใช้อินเทอร์เน็ตด้วยบริการตรวจสอบระยะไกล (RADIUS)

กรณีศึกษามหาวิทยาลัยนอร์ทกรุงเทพ

Ethernet User Accounts Management Using Remote Authentication Dial-In User Service (RADIUS)

Case Study of North Bangkok University

สุพจน์ พ่วงกำเหนิด¹

¹คณะเทคโนโลยีสารสนเทศ, มหาวิทยาลัยนอร์ทกรุงเทพ, suphot.ph@northbkk.ac.th

บทคัดย่อ

ในการเรียนการสอนปัจจุบันมีความจำเป็นต้องใช้งานอินเทอร์เน็ตเพื่อเป็นช่องทางในการสืบค้นข้อมูล และเป็นแหล่งในการจัดเก็บข้อมูลทางการศึกษา โดยในการเข้าใช้งานอินเทอร์เน็ตทุกครั้งผู้ให้บริการอินเทอร์เน็ตต้องเก็บ ข้อมูลจราจรคอมพิวเตอร์ (Log File) ให้ถูกต้องและเชื่อถือได้ และต้องเก็บไว้ไม่น้อยกว่า 90 วัน ตาม พรบ. คอมพิวเตอร์ 2550 และ 2560 ทางผู้วิจัยได้ทำการวิจัยในกรณีศึกษามหาวิทยาลัยนอร์ทกรุงเทพเป็น สถาบันอุดมศึกษาเอกชนที่ตั้งอยู่ในประเทศไทยมี 3 วิทยาเขตประกอบด้วยวิทยาเขตสะพานใหม่ วิทยาเขตรังสิต และศูนย์การศึกษานนทบุรี การยืนยันตัวตน (Authentication) ในขณะที่กำลังใช้งานระบบใดๆ บนเครือข่าย อินเทอร์เน็ต มีความจำเป็นต้องนำมาใช้งาน ให้ถูกต้องตาม กฎหมายดังกล่าว อีกทั้งยังพบปัญหาในการจัดการ บัญชีผู้ใช้งานอินเทอร์เน็ตที่มีทั้ง 3 วิทยาเขตให้สามารถเข้าใช้งานจากทุกวิทยาเขตได้ จากการศึกษาวิจัยผู้วิจัย พบว่าระบบที่สามารถนำไปใช้กับกรณีศึกษานี้ได้คือระบบ Remote Authentication Dial-In User Service (RADIUS) เป็นโพรโตคอลเครือข่ายปฏิบัติการบนพอร์ต 1812 ที่ให้การจัดการการรับรองความถูกต้องจากส่วนกลางการอนุญาต สำหรับผู้ใช้ที่เชื่อมต่อ และใช้บริการเครือข่าย RADIUS ได้รับการพัฒนาโดย Livingston Enterprises, Inc. ในปี 1991 ทางผู้วิจัยมีการติดตั้ง RADIUS Server เป็นศูนย์กลางในการจัดเก็บบัญชีผู้ใช้งานอินเทอร์เน็ต ทำให้การจัดการบัญชีผู้ใช้อินเทอร์เน็ตด้วยบริการตรวจสอบระยะไกล ทั้ง 3 วิทยาเขตสามารถจัดการบัญชีผู้ใช้งานได้อย่างมีประสิทธิภาพ และมีการเก็บข้อมูลจราจรคอมพิวเตอร์ (Log File) ตามกฎหมายดังกล่าว

คำหลัก: จัดการบัญชีผู้ใช้อินเทอร์เน็ตด้วยบริการตรวจสอบระยะไกล, การยืนยันตัวตน, จัดการระบบเครือข่ายคอมพิวเตอร์

Abstract

Nowadays, using the internet for teaching is mandatory. The internet can be used for information searching and also for storing educational data. Every time users have surfed the internet, the internet service provider has to store the log file correctly and trustworthily. The

log file must be kept for at least 90 days, according to the 2550 and 2560 Computer Acts. The researcher has chosen North Bangkok University as a case study. This is due to the fact that the North Bangkok University has 3 campuses including Saphanmai campus, Rangsit campus, and Nonthaburi Educational Center. The authentication of users using any system on the internet is essential to abide by the 2550 and 2560 Computer Acts. Moreover, the problem of internet users' management to correctly authenticate the user using the internet from any campus has also been found. Based on the study, the researcher has found that a suitable system for this case study is the Remote Authentication Dial-In User Service (RADIUS), which is the protocol operating on 1812 port that manages the authentication of connecting users from the center. RADIUS was developed by Livingston Enterprises, Inc. in 1991.

In this research, the RADIUS server has been installed as a center to manage internet accounts with the remote users' identification. In sum, RADIUS is an effective protocol to manage user's accounts among 3 campuses and helps to store the log file according to the 2550 and 2560 Computer Acts.

Keywords: Internet Accounts' Management with the Remote Authentication Dial-In User Service (RADIUS), Authentication, Computer Network Management.

ความเป็นมาและความสำคัญของปัญหา

มหาวิทยาลัยนอร์ทกรุงเทพเป็นสถาบันอุดมศึกษาเอกชนที่ตั้งอยู่ในประเทศไทยมี 3 วิทยาเขต ประกอบด้วยวิทยาเขตสะพานใหม่วิทยาเขตรังสิต และศูนย์การศึกษาเขตนนทบุรี [1] การเรียนการสอนจะต้องมีความจำเป็นในการแบ่งปันทรัพยากรกับทั้ง 3 วิทยาเขต การเรียนการสอนเป็นสิ่งจำเป็นในการใช้อินเทอร์เน็ต ในการค้นหาข้อมูลและปัญหาการเรียนรู้อื่น ๆ ในการใช้อินเทอร์เน็ตเกิดขึ้น 1) นักเรียนจะต้องเข้าสู่ระบบเพื่อใช้อินเทอร์เน็ตในทั้ง 3 วิทยาเขต และ 2) นักเรียนจะต้องมีชื่อผู้ใช้ในการเข้าถึงอินเทอร์เน็ตในมหาวิทยาลัยทั้ง 3 แห่ง จากปัญหาของนักเรียนที่เกิดจากการใช้งานระบบเข้าสู่ระบบอินเทอร์เน็ต นอกจากนี้ยังส่งผลให้ทรัพยากรสิ้นเปลืองเช่นต้องติดตั้งคอมพิวเตอร์โฮสต์สำหรับบริการทุกวิทยาเขต นักวิจัยศึกษารูปแบบของการรับรองความถูกต้องการจัดการเช่นระบบ Remote Authentication Dial-In User Service (RADIUS), [2] ซึ่งจะใช้ One Time Password (OTP), [3] ชื่อผู้ใช้และรหัสผ่านเพื่อเข้าสู่ระบบคลาวด์จากนอกเครือข่าย . สำหรับบริการการเข้าถึงเราจะใช้กลไกการเข้าถึงและควบคุมตามบทบาท Role Base Access Control (RBAC) [4] ผู้วิจัยพบว่าระบบที่สามารถนำไปใช้กับกรณีศึกษานี้ RADIUS เป็นโปรโตคอลเครือข่ายปฏิบัติการบนพอร์ต 1812 [5] ที่ให้การจัดการการรับรองความถูกต้องจากส่วนกลางการอนุญาตและการจัดการบัญชี (AAA หรือ Triple A) สำหรับผู้ใช้ที่เชื่อมต่อและใช้บริการเครือข่าย RADIUS ได้รับการพัฒนาโดย Livingston Enterprises, Inc. ในปี 1991 ในฐานะ

การรับรองความถูกต้องของเซิร์ฟเวอร์การเข้าถึงและโปรโตคอลการบัญชีและต่อมาได้นำเข้าสู่มาตรฐาน Internet Engineering Task Force (IETF) [6] เนื่องจากการสนับสนุนในวงกว้างและลักษณะที่แพร่หลายของโปรโตคอล RADIUS จึงมักถูกใช้โดยผู้ให้บริการอินเทอร์เน็ต (ISP) และองค์กรเพื่อจัดการการเข้าถึงอินเทอร์เน็ตหรือเครือข่ายภายในเครือข่ายไร้สายและบริการอีเมลครบวงจร เครือข่ายเหล่านี้อาจรวมโมเด็มสายสมาชิกดิจิทัล (DSL) จุดเชื่อมต่อเครือข่ายส่วนตัวเสมือน (VPN) พอร์ตเครือข่ายเว็บเซิร์ฟเวอร์ ฯลฯ [7] RADIUS เป็นโปรโตคอลไคลเอนต์/เซิร์ฟเวอร์ ที่ทำงานในเลเยอร์แอปพลิเคชัน และสามารถใช่ TCP หรือ UDP เป็นการขนส่ง เซิร์ฟเวอร์การเข้าถึงเครือข่ายเกตเวย์ที่ควบคุมการเข้าถึงเครือข่ายมักจะมีส่วนประกอบไคลเอนต์ RADIUS ที่สื่อสารกับเซิร์ฟเวอร์ RADIUS มักจะเป็นตัวเลือกแบ็คเอนต์สำหรับการตรวจสอบความถูกต้อง 802.1X เช่นกัน เซิร์ฟเวอร์ RADIUS มักจะเป็นกระบวนการพื้นหลังที่ทำงานบนเซิร์ฟเวอร์ UNIX หรือ Microsoft Windows [8]

วัตถุประสงค์

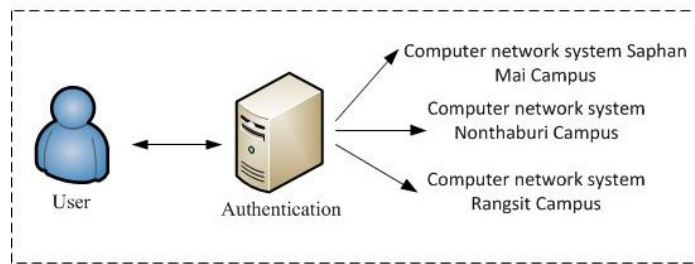
1. ออกแบบ และพัฒนาระบบการ ระบุตัวตนในการเข้าใช้งานเครือข่ายอินเทอร์เน็ตมหาวิทยาลัย นอร์ทกรุงเทพ
2. มีการเก็บข้อมูลจากรายการคอมพิวเตอร์ (Log File) ตาม พรบ. คอมพิวเตอร์ 2550 และ 2560
3. มีการประเมินประสิทธิภาพของระบบโดยผู้เชี่ยวชาญทางด้านเครือข่ายคอมพิวเตอร์
4. มีระบบ Authentication Dial-In User Service (RADIUS) กรณีศึกษามหาวิทยาลัยนอร์ทกรุงเทพ ที่สามารถใช้งานได้ทั้ง 3 วิทยาเขต

ประโยชน์ที่คาดว่าจะได้รับ

1. ได้ระบบ Authentication Dial-In User Service (RADIUS) กรณีศึกษามหาวิทยาลัยนอร์ทกรุงเทพ และมีการเก็บข้อมูลจากรายการคอมพิวเตอร์ (Log File) ตาม พรบ. คอมพิวเตอร์ 2550 และ 2560
2. ทำให้การจัดการบัญชีผู้ใช้อินเทอร์เน็ตด้วยบริการตรวจสอบระยะไกล ทั้ง 3 วิทยาเขตสามารถจัดการบัญชีผู้ใช้งานได้อย่างมีประสิทธิภาพ
3. ระบบมีประสิทธิภาพ โดยได้รับการประเมินประสิทธิภาพของระบบโดยผู้เชี่ยวชาญทางด้านเครือข่ายคอมพิวเตอร์

กรอบแนวคิด

ในการวิจัยครั้งนี้ผู้วิจัยทำการอธิบายถึงรูปแบบกรอบแนวคิดดังนี้ ตัวแปรต้น คือ ผู้ใช้งานทำการลงชื่อเข้าใช้งานระบบอินเทอร์เน็ตจากนั้น ตัวแปรตาม คือ ระบบที่ได้สามารถจัดการบัญชีผู้ใช้อินเทอร์เน็ตได้ทั้ง 3 วิทยาเขต



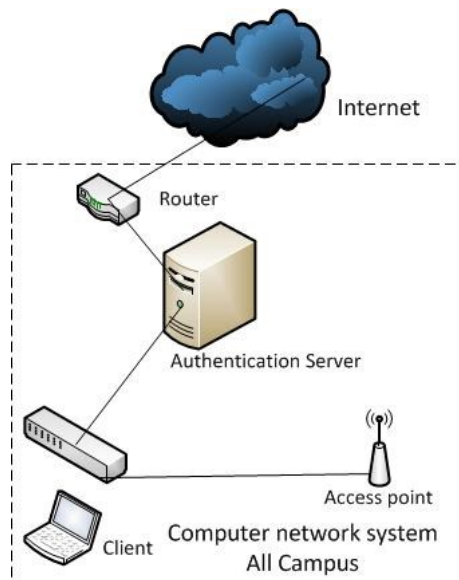
ภาพประกอบ 1 กรอบแนวคิดในการวิจัย

วิธีดำเนินการวิจัย

ในกระบวนการวิจัยมี 3 ขั้นตอนคือ 1) การศึกษาระบบเครือข่ายเก่า 2) การพัฒนาระบบเครือข่ายใหม่ 3) การประเมินประสิทธิภาพระบบเครือข่ายใหม่

1. การศึกษาระบบเครือข่ายเก่า

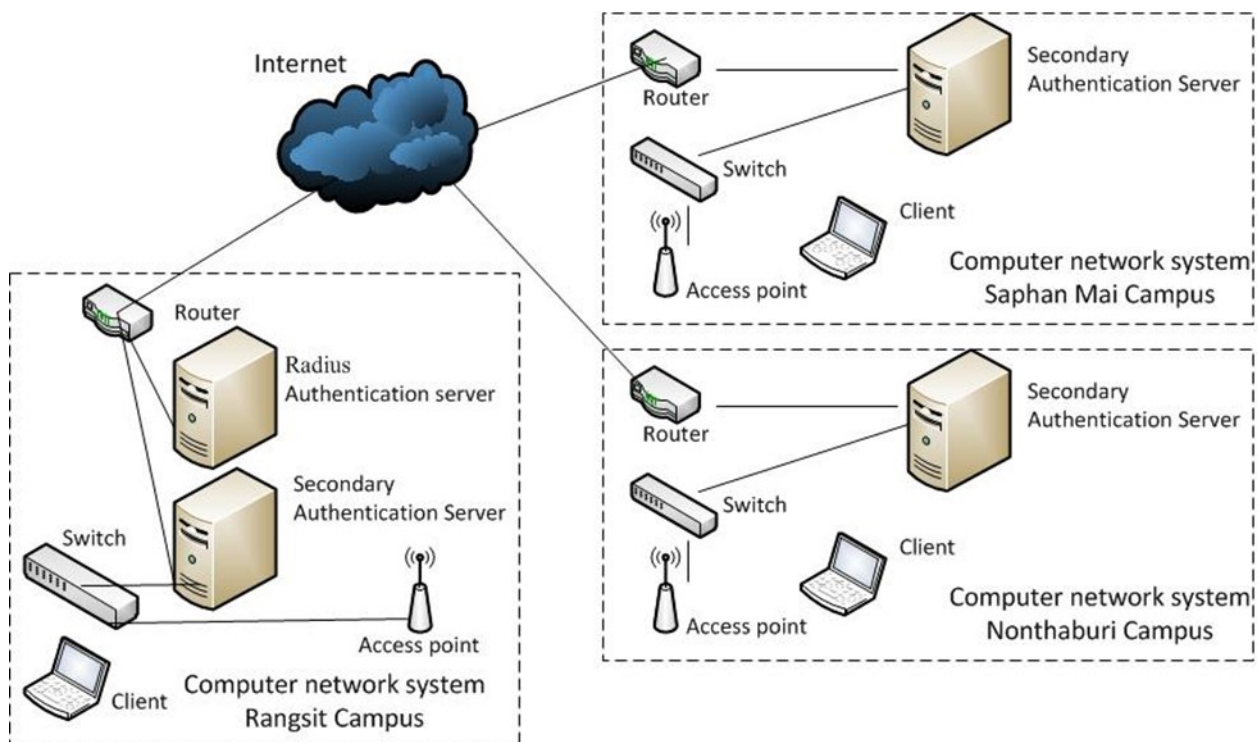
การศึกษาระบบเครือข่ายเก่าผู้วิจัยศึกษาปัญหาจากระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยนอร์ทกรุงเทพ พบว่ามหาวิทยาลัยนอร์ทกรุงเทพมี 3 วิทยาเขต แต่ละวิทยาเขตจะให้บริการอินเทอร์เน็ตแก่คณาจารย์ และนักศึกษา หากคนใดที่จะต้องมีชื่อผู้ใช้สำหรับการเข้าถึงอินเทอร์เน็ตบัญชีผู้ใช้อินเทอร์เน็ตจะถูกแยกออกจากทั้งสามวิทยาเขต หากนักศึกษาต้องการใช้อินเทอร์เน็ตในทุกวิทยาเขตนักศึกษาจะต้องมีชื่อผู้ใช้ในทุกวิทยาเขต ดังนั้นจากการศึกษาระบบเครือข่ายเก่าพบว่าปัญหาเกี่ยวกับบัญชีผู้ใช้อินเทอร์เน็ตเป็นหลัก ภาพประกอบ 2



ภาพประกอบ 2 ระบบเครือข่ายแบบเก่า

2. การพัฒนาระบบเครือข่ายใหม่

เมื่อเราทราบถึงปัญหาของระบบเครือข่ายเก่าผู้วิจัยจึงออกแบบระบบเครือข่ายโดยใช้คอมพิวเตอร์เพิ่มเติม 1 เครื่องติดตั้งที่วิทยาเขตรังสิตซึ่งเป็นวิทยาเขตหลักในการตรวจสอบความถูกต้อง และใช้ระบบปฏิบัติการ Linux Centos 7 และใช้ซอฟต์แวร์ daltoradius เพื่อทำเซิร์ฟเวอร์ Radius Authentication [11] ทุกวิทยาเขตมีเซิร์ฟเวอร์การตรวจสอบความถูกต้องรองที่ติดตั้ง Web Captive Portal การยืนยันตัวตนผ่าน Web Captive Portal เป็นอีกวิธีหนึ่งที่มีความนิยมอย่างสูงทั่วโลก และมี Solution ให้เลือกใช้มากมาย โดยผู้ใช้งานระบบเครือข่ายจะต้องทำการกรอก Username / Password ก่อนจึงจะทำการเข้าใช้งานระบบเครือข่ายได้ จึงสามารถยืนยันตัวตนบุคคลในการกระทำต่าง ๆ ได้อย่างน่าเชื่อถือในระดับหนึ่ง รวมถึงยังสามารถตกแต่งหน้า Web Captive Portal ให้สวยงามได้ ทำให้องค์กรดูมีความน่าเชื่อถือยิ่งขึ้น ดังนั้นสำหรับองค์กรนักศึกษาดังกล่าว ที่ต้องการการยืนยันตัวตนก่อนเข้าใช้งานระบบเครือข่ายด้วย Username และ Password การเลือกใช้ Web Captive Portal ก็ถือเป็นอีกหนึ่งทางเลือกที่ตอบโจทย์ได้อย่างตรงตัว โดยสำหรับองค์กรที่มีการยืนยันตัวตนที่ปลอดภัยกว่านี้ ก็อาจจะเลือกใช้ Web Captive Portal สำหรับผู้ใช้งานชั่วคราวหรือ Guest ก็ได้เช่นเดียวกัน



ภาพประกอบ 3 ระบบเครือข่ายแบบใหม่

จากภาพประกอบ 3 ระบบเครือข่ายคอมพิวเตอร์ทุกวิทยาเขตมีฟังก์ชันดังต่อไปนี้ เมื่อเครื่องไคลเอนต์เชื่อมต่อกับจุดเชื่อมต่อเซิร์ฟเวอร์การตรวจสอบความถูกต้องรองเป็นเครื่องที่ชื่อผู้ใช้งานรับรองความถูกต้องของนักเรียนโดย VPN (Virtual Private Network) ไปยังเซิร์ฟเวอร์ Radius Authentication data ชื่อผู้ใช้ทั้งหมด

3. การประเมินประสิทธิภาพของระบบเครือข่ายใหม่โดยผู้เชี่ยวชาญ

ในการประเมินประสิทธิภาพของระบบเครือข่ายใหม่โดยผู้เชี่ยวชาญ กำหนดให้มีการประเมินตามมาตรฐานการบริการจัดการเครือข่าย 5 ด้าน ดังนี้ 1) การบริหารประสิทธิภาพ (Performance Management) 2) การบริหารข้อผิดพลาด (Fault Management) 3) การบริหารการกำหนดค่าเบื้องต้น (Configuration Management) 4) การบริหารบัญชีผู้ใช้ (Accounting Management) และ 5) การบริหารด้านความปลอดภัย (Security Management)

3.1 การบริหารประสิทธิภาพ (Performance Management) มีจุดประสงค์หลัก คือ การทำบัญชี Host และอุปกรณ์ที่เกี่ยวข้อง ตรวจสอบ รายงาน วิเคราะห์ และควบคุมประสิทธิภาพ เช่น ปริมาณการใช้งาน และอัตราการส่งผ่านข้อมูล รวมถึง เส้นทางการรับ-ส่งข้อมูล (เน้นประสิทธิภาพโดยรวมของเครือข่าย)

3.2 การบริหารข้อผิดพลาด (Fault Management) มีจุดประสงค์หลัก คือ การเก็บประวัติ (log) การตรวจสอบ และแก้ไขข้อผิดพลาดต่าง ๆ ที่เกิดขึ้นในเครือข่าย โดยเน้นที่การแก้ไขปัญหาได้อย่างทันเวลา เช่น อุปกรณ์เครือข่ายชำรุด

3.3 การบริหารการกำหนดค่าเบื้องต้น (Configuration Management) มีจุดประสงค์หลัก คือ การบริหารค่าที่จะต้องกำหนดเบื้องต้น ของอุปกรณ์เครือข่าย เช่น IP Address, port no เป็นต้น

3.4 การบริหารบัญชีผู้ใช้ (Accounting Management) มีจุดประสงค์หลัก คือ การเก็บประวัติ (Log) การสร้าง การใช้งาน การควบคุมการใช้งานทรัพยากรเครือข่ายและอุปกรณ์ต่าง ๆ ของผู้ใช้งานเครือข่าย ซึ่งจะเกี่ยวข้องกับการกำหนดโควตา สิทธิการใช้งาน การจัดการบัญชีผู้ใช้ และกลุ่มผู้ใช้งานระบบก่อนจะเริ่มใช้งานระบบเครือข่าย จำเป็นต้องมีการกำหนดชื่อผู้ใช้งาน และกลุ่มผู้ใช้งานระบบ เพื่อให้ง่ายต่อการบริหารจัดการเครือข่าย และทำให้สามารถกำหนดสิทธิการใช้งานเครือข่ายได้ NOS ส่วนใหญ่จะสร้างบัญชีรายชื่อเบื้องต้นคือ Administrator, Guest ไว้ โดยผู้ดูแลระบบสามารถเพิ่มเติมแก้ไขบัญชีผู้ใช้ (User Account) รวมถึงกำหนดสิทธิการใช้งานเครือข่ายได้ ซึ่งจะเกี่ยวข้องกับการจัดการกลุ่มผู้ใช้ (Group Account) ตามความเหมาะสมของการทำงานได้

3.5 การบริหารจัดการด้านความปลอดภัย (Security Management) มีจุดประสงค์หลัก คือ การควบคุมการเข้าใช้ทรัพยากรเครือข่ายให้เป็นไปตามนโยบายที่ได้กำหนดไว้ ซึ่งจะเกี่ยวข้องกับ Firewall, Encrypt, Certificate Authority เป็นต้น

ขั้นตอนในการประเมินโดยผู้เชี่ยวชาญด้านระบบเครือข่ายคอมพิวเตอร์ 5 คน โดยผู้เชี่ยวชาญที่เชิญมาประเมินประสิทธิภาพของระบบเป็นผู้เชี่ยวชาญในด้านระบบเครือข่ายคอมพิวเตอร์ และสารสนเทศ ที่มีประสบการณ์ในด้านนี้โดยเฉพาะทำการประเมิน แบบประเมิน 5 ด้าน ที่กล่าวข้างต้น โดยใช้ scale 5 ระดับ หรือที่เรียกว่าวัดเจตคติตามเทคนิคของของ ลิเคิร์ท [9] (Likert technique) สถิติที่ใช้ คือ ค่าเฉลี่ย และค่าส่วนเบี่ยงเบนมาตรฐาน ซึ่งมีเกณฑ์กำหนดไว้ 2 แบบ คือ เกณฑ์การให้คะแนนและเกณฑ์การประเมิน

ผลการวิจัย

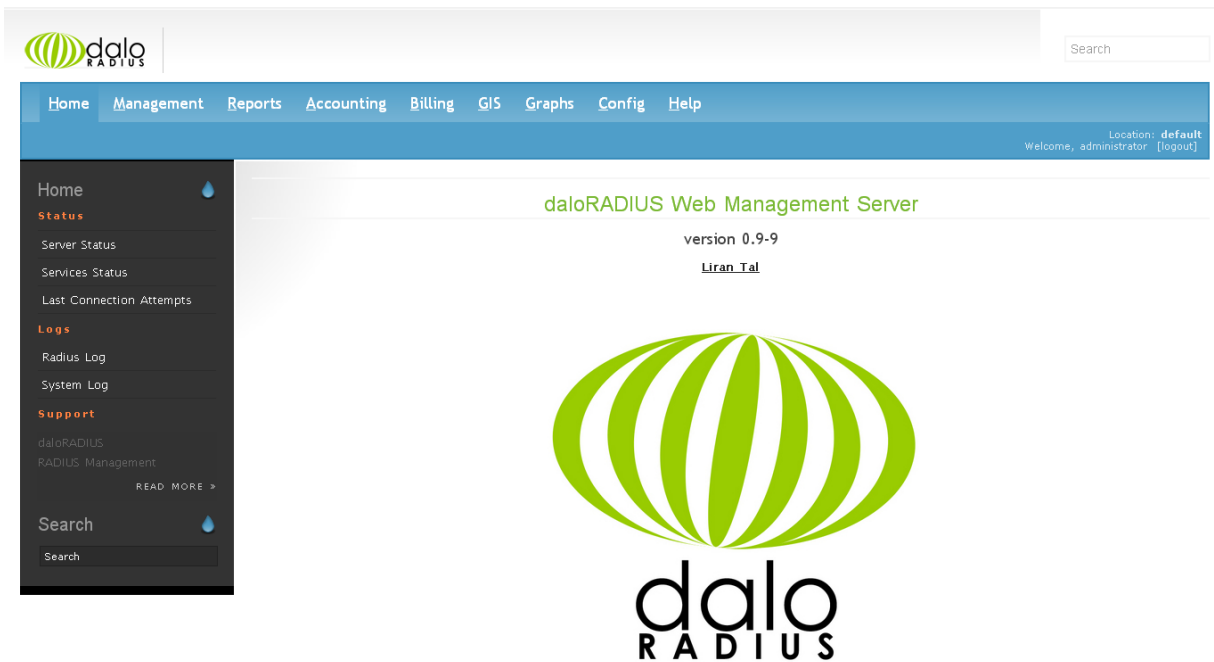
ผลการวิจัยประกอบด้วย 2 ส่วน คือ 1) ผลการวิจัยการติดตั้งระบบใหม่ และ 2) การประเมินประสิทธิภาพ โดยผู้เชี่ยวชาญระบบ

1. ผลการวิจัยของการติดตั้งระบบเครือข่ายใหม่

ผู้ใช้งานสามารถเข้าสู่ระบบเพื่อใช้อินเทอร์เน็ตจากมหาวิทยาลัย ด้วยบัญชีผู้ใช้เดียวจากหน้าจอรูปที่ 4 การรับรองความถูกต้องเข้าสู่ระบบผู้ใช้งานจะต้องป้อนชื่อผู้ใช้และรหัสผ่านเพื่อเข้าถึง มหาวิทยาลัยอินเทอร์เน็ต



ภาพประกอบ 4 หน้าจอการลงชื่อเข้าใช้งานอินเทอร์เน็ตแบบ Captive Portal



ภาพประกอบ 5 การตรวจสอบบัญชีผู้ใช้ระยะไกล แบบ dalo RADIUS

ตาราง 1 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และระดับความคิดเห็นผลของการประเมินประสิทธิภาพโดยผู้เชี่ยวชาญทางด้านระบบเครือข่าย

รายการประเมิน	ผลการประเมิน		
	\bar{X}	S.D.	แปลผล
1. Performance Management	4.76	0.87	Good
2. Fault Management	4.48	0.29	Good
3. Configuration Management	4.44	0.27	Good
4. Accounting Management	4.24	0.47	Good
5. Security Management	4.47	0.39	Good
Average sum	4.48	0.45	Good

สรุปผลการวิจัย

จากการวิจัยและพัฒนาระบบเครือข่ายในครั้งนี้ผู้วิจัยได้มีกระบวนการในการศึกษาปัญหาของระบบเครือข่ายแบบเก่าของกรณีศึกษา มหาวิทยาลัยนอร์ทกรุงเทพ โดยที่กรณีศึกษามีสถานที่ให้บริการอินเทอร์เน็ตทั้ง 3 วิทยาเขต และอยู่ต่างจังหวัดกันทั้งสิ้น ประกอบด้วย วิทยาเขตสะพานใหม่อยู่ที่ กรุงเทพฯ วิทยาเขตรังสิต อยู่ที่

จังหวัดปทุมธานี และศูนย์การศึกษานนทบุรีอยู่ที่จังหวัดนนทบุรี ทั้งนี้คณาจารย์และนักศึกษามีความจำเป็นต้องศึกษา หรือทำกิจกรรมต่างวิทยาเขต โดยหากมีการเชื่อมต่อระบบอินเทอร์เน็ต คณาจารย์และนักศึกษาที่จำเป็นต้องมีบัญชีผู้ใช้ในวิทยาเขตนั้น หากแต่ทางมหาวิทยาลัยทำการคัดลอกข้อมูลไว้ทุกวิทยาเขตก็จะทำให้เกิดขึ้นมูลซ้ำซ้อน และการบริหารจัดการบัญชีผู้ใช้งานอินเทอร์เน็ตของมหาวิทยาลัยเกิดความผิดพลาดได้ ผู้วิจัยจึงได้มีแนวคิดในการพัฒนาระบบเครือข่ายแบบใหม่ในการที่ต้องมีเครื่องแม่ข่ายในการจัดเก็บข้อมูลบัญชีผู้ใช้งานที่เดียว จึงพัฒนาระบบเครือข่ายที่มีการจัดการบัญชีผู้ใช้อินเทอร์เน็ตด้วยบริการตรวจสอบระยะไกล (RADIUS) เป็นศูนย์กลางในการตรวจสอบ โดยในแต่ละวิทยาเขตจะมี มีเซิร์ฟเวอร์การตรวจสอบความถูกต้องรองที่ติดตั้ง Web Captive Portal การยืนยันตัวตนผ่าน Web Captive Portal เครือข่าย จะต้องทำการกรอก Username / Password ก่อนจึงจะทำการเข้าใช้งานระบบเครือข่ายได้ จึงสามารถยืนยันตัวตนบุคคลในการกระทำต่างๆ ได้อย่างน่าเชื่อถือ ต่อมาผู้วิจัยได้ให้ผู้เชี่ยวชาญทางด้านระบบเครือข่ายทำการประเมินประสิทธิภาพของระบบ ทั้งหมด 5 คน โดยการประเมินได้ผลเป็น 5 หัวข้อดังนี้ 1) การบริหารประสิทธิภาพ (Performance Management) ค่าเฉลี่ย \bar{X} 4.76 S.D. 0.87 2) การบริหารข้อผิดพลาด (Fault Management) ค่าเฉลี่ย \bar{X} 4.48 S.D. 0.29 3) การบริหารการกำหนดค่าเบื้องต้น (Configuration Management) ค่าเฉลี่ย \bar{X} 4.44 S.D. 0.27 4) การบริหารบัญชีผู้ใช้ (Accounting Management) ค่าเฉลี่ย \bar{X} 4.24 S.D. 0.47 และ 5) การบริหารด้านความปลอดภัย (Security Management) ค่าเฉลี่ย \bar{X} 4.47 S.D. 0.39 โดยการประเมินผลรวมของค่าเฉลี่ย \bar{X} 4.48 S.D. 0.45 แปรผลอยู่ในระดับดี งานวิจัยที่พัฒนาขึ้นสามารถรองรับการจัดการเก็บข้อมูลจราจรคอมพิวเตอร์ (Log File) ให้ถูกต้องและเชื่อถือได้ 90 วัน ตาม พรบ. คอมพิวเตอร์ 2550 และ 2560 และระบบสามารถจัดการบัญชีผู้ใช้อินเทอร์เน็ตด้วยบริการตรวจสอบระยะไกล (RADIUS) กรณีศึกษา มหาวิทยาลัยนอร์ทกรุงเทพ ใช้งานได้ในปัจจุบัน

อภิปรายผล

งานวิจัยนี้มีการนำเอาเทคโนโลยีหลักที่ใช้ในการ Authentication การยืนยันตัวตนเพื่อเข้าใช้ระบบเครือข่าย แบบ Web Captive Portal การยืนยันตัวตนผ่าน Web Captive Portal ถือเป็นอีกวิธีหนึ่งที่ได้รับคามนิยมอย่างสูงทั่วโลก และมี Solution ให้เลือกใช้มากมาย โดยผู้ใช้งานระบบเครือข่ายจะต้องทำการกรอก Username / Password ก่อนจึงจะทำการเข้าใช้งานระบบเครือข่ายได้ จึงสามารถยืนยันตัวตนบุคคลในการกระทำต่าง ๆ ได้อย่างน่าเชื่อถือในระดับหนึ่ง ดังนั้นการเข้าใช้งานอินเทอร์เน็ตต้องการยืนยันตัวตนก่อนเข้าใช้งานระบบเครือข่ายด้วย Username และ Password ในทุกวิทยาเขต พร้อมกับการใช้เทคโนโลยี Remote Authentication Dial-In User Service (RADIUS) โดยมีความสอดคล้องกับงานวิจัยของ [10] Don Wipa and Chatchawin Namman ที่พัฒนาระบบโดยใช้โดยใช้โปรโตคอล RADIUS สำหรับโรงเรียน แต่ทางโรงเรียนมีวิทยาเขตเดียว ในที่นี้ทางผู้วิจัยพัฒนาขึ้นใช้โปรแกรม freeradius เป็นตัวจัดการในเรื่องของการพิสูจน์ตัวตน โดยโปรแกรม freeradius มีหน้าที่หลัก 3 อย่างคือ การตรวจสอบ Username และ Password (Authentication) การกำหนดสิทธิ์ ในการเข้าใช้งานของผู้ใช้ (authorization) การเก็บข้อมูล รายละเอียดการใช้งานของผู้ใช้

(Accounting) RADIUS ที่กล่าวมานี้ถูกติดตั้งที่จุดเดียวคือวิทยาเขตรังสิต ระบบสามารถตอบสนองการให้บริการได้อย่างดีตามที่ได้รับการประเมินจากผู้เชี่ยวชาญทางด้านระบบเครือข่าย

ข้อเสนอแนะ

ในการพัฒนางานวิจัยระยะต่อไปทางผู้วิจัยมีแนวคิดที่จะให้มี 1) การลงทะเบียนการเข้าใช้งานอินเทอร์เน็ต มีระบบการตรวจสอบอัตโนมัติ 2) เชื่อมฐานข้อมูลรหัสนักศึกษาเพื่อเป็นฐานข้อมูลในการใช้งานต่อไป เพื่อเพิ่มความปลอดภัย 3) ควรมีการลงทะเบียน MAC Address และ 4) เรื่องการเตรียมการในการสำรองข้อมูลบัญชีผู้ใช้งานอินเทอร์เน็ตต่อไปในกรณีเกิดไฟฟ้าขัดข้อง

กิตติกรรมประกาศ

ผู้วิจัยขอขอบคุณมหาวิทยาลัยนอร์ทกรุงเทพที่ให้ทุนสนับสนุนการทำวิจัยในครั้งนี้ ขอขอบคุณคณะทำงานแผนกสารสนเทศ สำนักหอสมุดและสารสนเทศที่ให้ข้อมูลในการรวบรวมทำวิจัยครั้งนี้

เอกสารอ้างอิง

- [1] มหาวิทยาลัยนอร์ทกรุงเทพ. (2562 มกราคม 12). *เกี่ยวกับมหาวิทยาลัยนอร์ทกรุงเทพ* [ออนไลน์]. แหล่งที่มา: <http://www.northbkk.ac.th/about.php>
- [2] Md.Hashmathur Rehman Dr.A. Govardhan T. Venkat Narayana Rao, *Design and Implementation of RADIUS-An Network Security Protocol*, 48Vol. 10 Issue 7 Ver.1.0 September 2014
- [3] A. Aboshosha, K. A. ElDahshan, E. K. Essayed and A. A. Elngar, "Multi-Channel User Authentication Protocol based on Encrypted Hidden OTP", *International Journal of Computer Science and Information Security*, vol. III, pp. 14-19, June 2015
- [4] David Ferraiolo; (NIST), Author: Richard Kuhn (1992-10-13). "Role-Based Access Controls". [Csrc.nist.gov](http://csrc.nist.gov). pp. 554-563. Retrieved 15 August 2018.
- [5] *Network Authentication, Authorization, and Accounting: Part One -The Internet Protocol Journal-Volume 10, No. 1 -Cisco.* [Online]. Available: <https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-35/101-aaa-part1.html>. [Accessed: 03-Jul-2018
- [6] "Internet Engineering Task Force (IETF)". *RIPE Network Coordination Centre*. August 10, 2012. Retrieved August 22, 2018.
- [7] Tarek S. Sobh, Yasser Aly. Effective and Extensive Virtual Private Network. *Journal of Information Security*, 2011, 2, 39-49

[8] Linuxfx, "Linuxfx Computing," 2012. [Online] .Available: <http://linuxfx.sdf.org/ubuntu.html>.

[9] Likert, Rensis A. (1961). *New Patterns of Management*. New York: McGraw-Hill Book Company Inc.

[10] Don Wipa and Chatchawin Namman, "Internet Management System Using RADIUS Protocol", *วารสารวิชาการและวิจัย มทร.พระนคร*, ปีที่ 11, ฉบับที่ 2, หน้า 99 - 111 , กรกฎาคม-ธันวาคม 2560