**ระบบเฝ้าติดตามการจราจรบนระบบเครือข่าย**

**Monitoring Traffic System on the Network**

**บทคัดย่อ**

โครงงานพิเศษจัดทำระบบเฝ้าติดตามการจราจรบนระบบเครือข่ายโดยใช้ความรู้ด้าน Network เรื่องโปรโตคอล SNMP ในการตรวจสอบค่าการทำงานของอุปกรณ์เครือข่าย และ ใช้ความรู้ในการเขียนโปรแกรมเบื้องต้น เพื่อใช้พัฒนาหน้าเว็บบราวเซอร์เพื่อใช้ในการติดตามการทำงานของระบบเครือข่าย และแจ้งเตือนผู้ใช้งานเมื่อเกิดความผิดปกติขึ้นกับระบบเครือข่าย เนื่องจากปัจจุบันทางคณะเทคโนโลยีและการจัดการอุตสาหกรรมยังไม่มีระบบที่ใช้ตรวจสอบระบบเครือข่าย ทำให้มักพบปัญหาเรื่องอุปกรณ์เกิดชำรุดเสียหาย ส่งผลกับการทำงานของระบบเครือข่ายระบบเกิดความเสียหายและใช้งานไม่ได้ชั่วคราว เนื่องจากไม่มีการตรวจสอบ ตรวจพบปัญหาเมื่อระบบเสียหายแล้ว ดังนั้นทางผู้จัดทำจึงพัฒนาระบบเฝ้าติดตามการจราจรบนระบบเครือข่ายขึ้นเพื่อเฝ้าติดตามและตรวจสอบการทำงานของระบบเครือข่ายรวมไปถึงการแจ้งเตือนเมื่อเครือข่ายมีการทำงานผิดพลาด หรืออุปกรณ์มีการทำงานผิดปกติ ระบบจะมีการแจ้งเตือนเพื่อแก้ไขปัญหาได้ทันเวลา ลดความเสียหายที่จะเกิดขึ้นได้

**ABSTRACT**

This thesis was created for monitoring network by using knowledge about the network in SNMP Protocol. To make sure that a network device is working and using fundamental of programming for make website to follow monitoring of the network, then notification to the user about a problem in the network. At present, Faculty of Industrial Technology and Management still not have network monitoring so, when device broken will impact to network system, it will make network have a problem for temporary because the network have no monitoring. Therefore, this thesis was developed for monitoring network in Faculty of Industrial Technology and Management including notification to user when the network was failing so, damage can reduce.

**คำสำคัญ –** Network, Network Monitoring, SNMP

**1. บทนำ**

ปัจจุบันเทคโนโลยีมีการพัฒนาเพิ่มมากขึ้น และเริ่มมีการใช้ Internet ในการติดต่อสื่อสารมากขึ้น เมื่อระบบเครือข่ายได้เข้ามามีความสำคัญมากขึ้น จึงจำเป็นต้องมีการดูแลระบบเครือข่ายเพื่อให้สามารถ ทำงานได้ตลอดเวลาและมีประสิทธิภาพ โดยการเฝ้า ดูแลและการบริการระบบเครือข่าย (Network Monitoring) เพื่อจะคอยตรวจสอบสภาพเครือข่ายให้มีความเสถียร ปลอดภัย ตรวจสอบการทำงานของเครือข่าย และคอยบันทึกสถานะการทำงาน และคอยแจ้งเตือนให้ผู้ดูแลทราบ

ดังนั้นวัตถุประสงค์ของโครงการพิเศษเพื่อแสดงสถานะของอุปกรณ์เครือข่าย เพื่อใช้ในการจัดการและพัฒนาระบบให้มีประสิทธิภาพมากขึ้น ข้อมูลที่ได้จะนำไปเป็นแนวทางในการแก้ไขปัญหาได้รวดเร็วและเกิดความเสียหายน้อยลง โดยการนำข้อมูล Traffic ทั้งหมดมาวิเคราะห์แล้วทำการแจ้งเตือนเมื่อพบสิ่งผิดปกติที่เกิดขึ้นบนเครือข่าย และระบบยังมีการนำเสนอข้อมูลให้สามารถเปรียบเทียบความแตกต่างของเหตุการณ์บนเครือข่ายได้

**2. เอกสารที่เกี่ยวข้อง**

**2.1 Network Monitoring**

Network Monitoring คือ การเฝ้าระวังระบบเครือข่ายเพื่อไม่ให้เกิดความเสียหายต่อระบบโดยการเฝ้าระวังการทำงานของระบบเครือข่ายและคอยบันทึกสถานะ การทำงานต่าง ๆ ของแต่ละอุปกรณ์ในเครือข่ายและสามารถแจ้งเตือนให้ผู้ดูแลระบบรับรู้ หากมีส่วนใดส่วนหนึ่งเกิดทำงานผิดพลาด เช่น เครือข่ายช้าผิดปกติ หรือ หน้าเว็บไซต์ไม่สามารถเข้าถึงได้เป็นต้น ซึ่งเมื่อพบข้อผิดพลาดก็จะสามารถแก้ไขได้ทันท่วงทีก่อนที่ระบบจะมีปัญหามากขึ้นจนนำไปสู่ความเสียหายทั้งระบบ นอกจากนี้จะช่วยให้สามารถดูแลอุปกรณ์ Network จำนวนมากที่อยู่ในพื้นที่เดียวกันได้ทั่วถึง หรืออยู่ห่างออกไปได้อย่างครอบคลุม

**2.2 โปรโตคอล SNMP**

Simple Network Management Protocol (SNMP) เป็นโปรโตคอลที่ประยุกต์เพื่อใช้ในการกำหนดรูปแบบและวิธีการจัดการเครือข่าย โดยจะใช้ SNMP ในการดูค่าการทำงานของอุปกรณ์ต่าง ๆ ปัจจุบันโปรโตคอล SNMP ถูกนำมาใช้ในการจัดการอุปกรณ์ ต่าง ๆ เช่น เครื่องแม่ข่าย ไฟร์วอลล์ เราเตอร์ สวิตซ์ ในระบบเครือข่ายโปรโตคอล SNMP ช่วยให้ผู้ดูแลระบบเครือข่ายสามารถรวบรวมข้อมูล เพื่อนำไปวิเคราะห์ค้นหาปัญหาและแก้ไขปัญหาความผิดพลาดของระบบเครือข่ายที่เกิดขึ้นอีกทั้งใช้ในการจัดการประสิทธิภาพและการวางแผนการพัฒนาของระบบเครือข่ายองค์กรในอนาคต

**2.3 หมายเลข OID**

หมายเลข OID คือชุดของตัวเลขที่คั่นด้วยเครื่องหมายจุดเพื่อแยกแยะหาตำแหน่ง ในแต่ละตัวเอเยนต์จะมีฐานข้อมูลที่เป็นเสมือนกับสมุดบันทึกตำแหน่งของออบเจ็กต์ทั้งหมดรวมทั้งหมายเลขและชื่ออ้างอิงที่เรียกว่า MIB (Management Information Base) โดยที่ MIB จะจัดเรียงชื่อ, หมายเลข OID, ชนิดข้อมูล, สิทธิการอ่านและเขียนรวมทั้งคำอธิบายสั้น ๆ สำหรับแต่ละออบเจ็กต์ที่อยู่ในตัวเอเยนต์

**2.4 Google Sheets**

Google Sheets นำมาใช้ในการเก็บข้อมูล Log แทนการจัดเก็บลง Database เพื่อลดค่าใช้จ่ายในการติดตั้งเครื่อง Server ลดค่าซ่อมบำรุง ลดความเสียหายที่อาจจะเกิดขึ้นกับเครื่อง Server และยังใช้งานสะดวกมีพื้นที่จัดเก็บเพียงพอ สามารถดูข้อมูลจากที่ไหนก็ได้ ผู้ใช้สามารถเข้าถึงได้จากคอมพิวเตอร์ทุกเครื่อง ผ่านเว็บบราวเซอร์

**2.5 API**

**API**[(](http://www.xn--12cg1cxchd0a2gzc1c5d5a.net/%E0%B8%95%E0%B8%B1%E0%B8%A7%E0%B8%A2%E0%B9%88%E0%B8%AD-%E0%B8%84%E0%B8%B3%E0%B8%A2%E0%B9%88%E0%B8%AD-%E0%B8%84%E0%B8%B3%E0%B8%AA%E0%B8%B1%E0%B9%89%E0%B8%99/)**Application Programming Interface**) เป็นช่องทางการเชื่อมต่อระหว่างเว็บไซต์หนึ่งไปยังอีกเว็บไซต์หนึ่ง หรือเป็นการเชื่อมต่อระหว่าผู้ใช้งานกับ Server หรือจาก Server เชื่อมต่อไปหา Server ซึ่ง API นี้เปรียบได้เป็น[ภาษา](http://www.xn--12cg1cxchd0a2gzc1c5d5a.net/%E0%B8%A0%E0%B8%B2%E0%B8%A9%E0%B8%B2%E0%B8%AD%E0%B8%B2%E0%B9%80%E0%B8%8B%E0%B8%B5%E0%B8%A2%E0%B8%99/)คอมพิวเตอร์ที่ทำให้คอมพิวเตอร์สามารถสื่อสารและแลกเปลี่ยนข้อมูลกันได้อย่างอิสระ โดยจะใช้ API ทำหน้าที่ช่วยในการเข้าถึงข้อมูลต่าง ๆ หรือจะเป็นการนำข้อมูลต่าง ๆ ออกจากเว็บไซต์ หรือจะเป็นการส่งข้อมูลเข้าไปก็ได้ โดยเจ้าของเว็บไซต์ที่มี API จะกำหนดขอบเขตในการเข้าถึงบริการต่าง ๆ ของทางเว็บไซต์

**3. ขั้นตอนการพัฒนาและการออกแบบระบบ**

**3.1 ขั้นตอนการค้นคว้าและเก็บรวบรวมข้อมูล Log**

ขั้นตอนการค้นคว้าข้อมูลการเก็บ Log การศึกษาเรื่องโปรโตคอล SNMP เพื่อนำมาใช้ในการเก็บ Log จากอุปกรณ์ภายในเครือข่าย ศึกษาข้อมูลเรื่องเลข MIB ที่ใช้ในการดึงข้อมูลต่าง ๆ ของอุปกรณ์ และวิธีการใช้เลข MIB เพื่อดึงข้อมูล การศึกษาการใช้ Google Sheets และวิธีการนำข้อมูลขึ้น Google Sheets และศึกษาการแปลงข้อมูลจาก Google Sheets เป็น API เพื่อนำไปใช้แสดงผลหน้าเว็บบราวเซอร์ รวมไปถึงการดึง API ไปใช้ต่อ ขั้นตอนก่อนการเก็บข้อมูล Log จะทำการทดสอบอ่านค่าจาอุปกรณ์ผ่านโปรแกรม เพื่อทดสอบเรียกค่าโอไอดี ที่ต้องการขึ้นมาตรวจสอบก่อนทำการเก็บค่าจริง

**3.2** **การออกแบบการจัดเก็บข้อมูล**

การออกแบบการจัดเก็บข้อมูล Text ธรรมดา ๆ ที่ถูกจัดเรียงให้อยู่ในรูปแบบของ Object Array โดยใช้เครื่องหมาย [ ] แทน Array และ { } แทน Hash (หรือ Associative Array)เขียนคร่อมข้อมูลไว้ภายใน ซึ่งเป็นการกำหนดคุณสมบัติให้กับวัตถุด้วยการสร้างวัตถุที่เป็นข้อมูลขึ้นมา ในรูปแบบของ JSON **เพื่อทำการส่งค่าไปยัง Google Sheets** ทำให้การเขียนโปรแกรมที่ทำการส่งค่าระหว่าง **Server** กับ **Client** นั้นสะดวกยิ่งขึ้น จะเพิ่มความสามารถในการส่งค่าตัวแปร ระหว่างกันได้ดียิ่งกว่าเดิม เพราะ **JSON** Code เป็น String ที่มีรูปแบบง่าย ๆ สามารถอ่านและเข้าใจได้ง่าย อีกทั้งในฝั่งของ **Client และ Server** ก็สามารถแปลงค่าจาก **JSON** ได้อย่างไม่ยากเช่นเดียวกัน โดยข้อมูลจะถูกจัดเก็บใน Google Sheets ในรูปแบบของตาราง ที่มี Row และ Colum ใน Row จะแทนด้วย Key และใน Colum จะแทน Value

**3.3 การออกแบบหน้าจอเมนูเริ่มต้นของเว็บ**

การออกแบบหน้าจอเมนูเริ่มต้นของเว็บนั้นได้ออกแบบให้ดูเรียบง่าย ทำให้เห็นเมนูได้อย่างชัดเจน ในหน้าจอเมนูเริ่มต้นจะมีแถบเมนู 6 ส่วนคือ Dashboard, Device, Interface และTop 10 Ranking ใน Dashboard เมื่อกดเข้าไปจะพบสถานะของอุปกรณ์และกราฟแสดง Internet Traffic เป็นต้น ในส่วนของ Device เป็นเมนูที่แสดงรายละเอียดของอุปกรณ์ จัดวางตำแหน่งให้ดูเรียบง่าย และใช้รูปภาพสื่อถึงข้อมูลได้อย่างชัดเจน รวมถึงรายะเอียดของแต่ละอุปกรณ์ ดังนี้ ชื่ออุปกรณ์ IOS version หมายเลขไอพี สถานะของตัวอุปกรณ์ Uptime รวมถึงกราฟ Traffic ในส่วนของ Interface เป็นเมนูที่แสดงรายชื่ออุปกรณ์ เมื่อกดเลือกอุปกรณ์ จะมีเมนูย่อยเป็นรายชื่อ Interface เมื่อกดเลือกรายชื่อ Interface จะแสดงกราฟ Traffic และแสดงสถานะของแต่ละ Interface ได้ชัดเจน ในส่วนของ Top 10 Ranking เป็นส่วนแสดง 10 อันดับ Network ที่มีการใช้งานสูงสุด 10 อันดับ พร้อมแสดงข้อมูลเป็นตารางด้านล่างของกราฟ

**3.4** **การออกแบบส่วนติดต่อกับผู้ใช้**

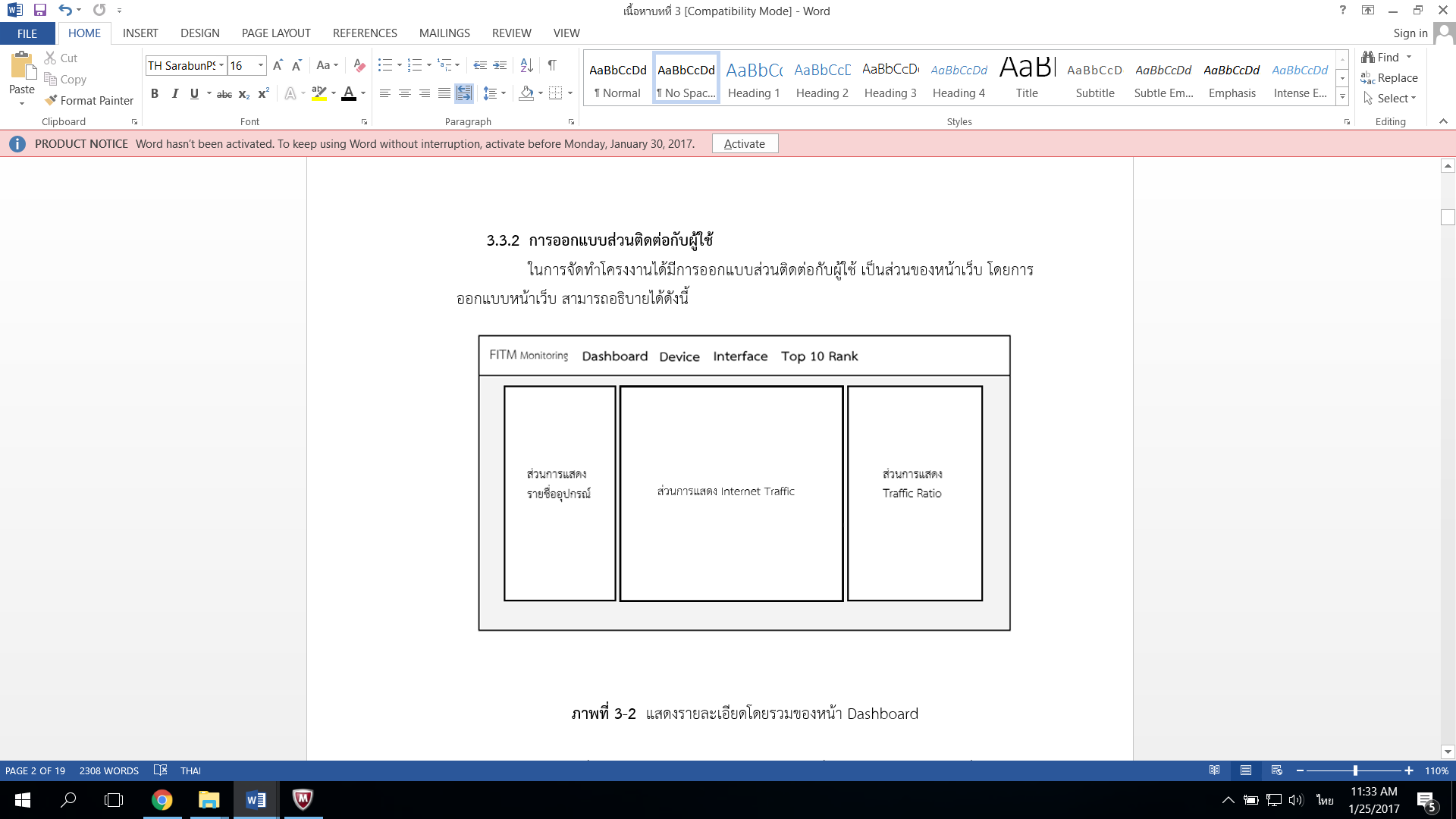
ในการจัดทำโครงงานได้มีการออกแบบส่วนติดต่อกับผู้ใช้ เป็นส่วนของหน้าเว็บ โดยเมื่อเข้าหน้าเว็บแอพพลิเคชั่นหน้าแรก จะพบข้อมูลที่แสดงข้อมูลโดยรวมของสถานะของเครือข่าย โดยจะมีรายละเอียดดังนี้ แถบด้านบน เป็นเมนูที่จะนำไปสู่หน้าต่างอื่น ๆ เพื่อแสดงข้อมูลที่ละเอียดมากขึ้น โดยจะแบ่งออกเป็น 4 เมนูหลัก เช่น

3.4.1 ส่วนของหน้า Dashboard เป็นเมนูแสดงข้อมูลโดยรวมของสถานะเครือข่าย

3.4.2 ส่วนของหน้า Device เป็นเมนูหลักที่ 2 โดยจะมีเมนูย่อย เป็นรายชื่ออุปกรณ์ทั้ง 6 เครื่อง โดยสามารถเลือกดูรายละเอียดของอุปกรณ์ได้จากเมนูนี้

3.4.3 ส่วนของหน้า Interface เป็นเมนูหลักที่ 3 โดยจะมีเมนูย่อยเป็นรายชื่ออุปกรณ์ทั้ง 6 เครื่อง โดยสามารถเลือกอุปกรณ์ที่ต้องการ และเมื่อเข้าไปในรายชื่ออุปกรณ์จะมีเมนูย่อย เป็นรายชื่อ Interface โดยสามารถเลือกดูรายละเอียดของ Interface ได้จากเมนูนี้

3.4.4 ส่วนของหน้า Top 10 Ranking เป็นเมนูหลักที่ 4 โดยแสดงอันดับ VLAN ที่มีการใช้งานสูงสุด



รูปที่ 1.แสดงรายละเอียดโดยรวมของหน้า Dashboard

**4. ผลการดำเนินงาน**

การดำเนินการจัดทำโครงงานพิเศษ ซึ่งหลังจากการศึกษาเรียนรู้เกี่ยวกับข้อมูลที่เกี่ยวข้องกับการทำระบบเฝ้าติดตามการจราจรบนระบบเครือข่าย เริ่มดำเนินการเก็บค่า Log ของทุก ๆ อุปกรณ์จะได้ข้อมูลที่ผ่านกระบวนการเตรียมข้อมูล(Preprocessing) เรียบร้อยแล้วจะได้เป็นข้อมูลชุดสุดท้ายที่จะนำไปจัดเก็บลง Google Sheets เพื่อเตรียม API ที่จะนำไปใช้นำเสนอผ่านหน้าเว็บ แอพพลิเคชั่นตามที่ได้ออกแบบไว้ข้างต้น ในการจัดทำโครงงานพิเศษได้มีกำหนด และวางแผนการดำเนินงานเพื่อให้การดำเนินงานสำเร็จตรงตามระยะเวลาที่กำหนดไว้ และตรงตามวัตถุประสงค์ของโครงงานที่ได้กำหนดไว้

**5. สรุปผลการดำเนินการ**

**5.1 สรุปผลการดำเนินงาน**

จากการจัดทำโครงงานพิเศษ ระบบเฝ้าติดตามการจราจรบนระบบเครือข่าย ของคณะเทคโนโลยีและการจัดการอุตสาหกรรม โดยทำการตั้งเครื่องคอมพิวเตอร์สำหรับทำการเก็บ Log การทำงานของอุปกรณ์ทั้งหมด 6 เครื่อง ได้แก่ SW4503, R101C, R415, Rshop, R330A และ R124 การเก็บค่าจะทำการจัดเก็บทุก ๆ 5 นาที เพื่อให้เห็นการเปลี่ยนแปลงของสถานะของเครือข่ายได้ชัดเจน ข้อมูลจาก Log จะถูกคัดเหลือแต่ข้อมูลที่ต้องการนำไปใช้ เพื่อจัดเก็บลง Google Sheets เตรียม API ที่ไว้ใช้แสดงในส่วนของหน้าของเว็บแอพพลิเคชั่น ทำการดึง API มาแสดงผลที่หน้าเว็บแอพพลิเคชั่น ผ่าน Sheetsu จะได้ข้อมูลเป็น Object โดยมีการแสดงผลในรูปแบบที่เหมาะสม เช่น ข้อมูล Traffic ขาเข้าและขาออกแสดงผลในรูปแบบของกราฟเส้น และ กราฟแท่ง แสดงอัตราส่วนของ Traffic แสดงเป็นกราฟวงกลม และข้อมูลที่เป็นลำดับ Network ที่มีการใช้งานสูงสุด 10 อันดับจะแสดงผลในรูปแบบของตารางเพื่อให้ดูง่าย การออกแบบหน้าเว็บแอพพลิเคชั่นให้ใช้งานง่าย มีรูปภาพอุปกรณ์และใช้สีแสดงสถานะที่มีความผิดปกติ เมื่อทดสอบการทำงานของระบบ ประโยชน์ที่ได้รับ คือ สามารถนำข้อมูลที่ได้มาวิเคราะห์และประเมินประสิทธิภาพการทำงานของระบบเครือข่ายได้ ผู้ดูแลระบบสามารถเฝ้าดู (Monitoring) ภาพรวมของระบบเครือข่ายและมีการแจ้งเมื่อมีการทำงานผิดพลาด ส่งผลให้ผู้ดูแลระบบสามารถแก้ไขปัญหาได้อย่างรวดเร็วและมีประสิทธิภาพมากยิ่งขึ้น

**5.2 ปัญหาอุปสรรคและแนวทางการแก้ไข**

จากการที่ได้เริ่มพัฒนาเว็บแอพพลิเคชั่นตั้งแต่ขึ้นตอนการศึกษาการทำจนกระทั่งเสร็จมีปัญหาที่เกิดขึ้นกับการทำเว็บแอพพลิเคชั่น ดังนี้

5.2.1 ปัญหาของการเก็บข้อมูลขึ้น Google Sheets ที่ต้องผ่าน Sheetsu ที่ใช้แปลงเป็น API มีข้อจำกัดทางด้านปริมาณในการใช้งาน

แนวทางการแก้ไขปัญหา

โดยการเปลี่ยน Url ที่ใช้ดึงข้อมูลขึ้นชีท

5.2.2 ปัญหาในการดึง API ใช้เวลานานเมื่อข้อมูลมีปริมาณข้อมูลจำนวนมาก

แนวทางการแก้ไขปัญหา

โดยการดึงข้อมูลแค่บางข้อมูลที่ต้องการแสดงผลเท่านั้น

**5.3 ข้อเสนอแนะ**

ข้อเสนอแนะหลังจากศึกษาและเริ่มพัฒนาระบบเฝ้าติดตามการจราจรบนระบบเครือข่ายของคณะเทคโนโลยีและการจัดการอุตสาหกรรม ควรจะศึกษาข้อมูลเกี่ยวกับอุปกรณ์เครือข่ายให้มากขึ้น เนื่องจากแต่ละอุปกรณ์มีข้อมูลการทำงานในฐานข้อมูลที่แตกต่างกัน และมีข้อจำกัด ควรศึกษาระบบ Monitoring หลาย ๆ ระบบเพื่อดูข้อดีและข้อเสียเพื่อนำมาพัฒนาระบบให้มีประสิทธิภาพมากยิ่งขึ้น ควรศึกษาระบบ Monitoring เนื่องจากระบบที่พัฒนาขึ้นมีความจำกัดในเรื่องเวลาในการทำงาน จึงทำให้ระบบมีประสิทธิภาพไม่ดีเท่าที่ควร จึงมีแนวคิดที่จะพัฒนาระบบต่อไปในอนาคตเพื่อให้ระบบทำงานได้ดียิ่งขึ้น โดยมีแนวทางในการพัฒนาในอนาคต มีดังนี้

**เอกสารอ้างอิง**

[1] ทดสอบการแปลงหน่วยข้อมูล. [ออนไลน์]. แหล่งที่มา: [http://www.endmemo.com/sconvert/bpsgbps.php 15 สิงหาคม 2559](http://www.endmemo.com/sconvert/bpsgbps.php%20%20%20%2015%20สิงหาคม%202559)

[2] อัตราหน่วยข้อมูล. [ออนไลน์].แหล่งที่มา: <https://th.wikipedia.org/wiki/หน่วยอัตราข้อมูล>

13 สิงหาคม 2559

[3] BootstrapCDN. [ออนไลน์]. แหล่งที่มา:

<https://www.bootstrapcdn.com/>

15 สิงหาคม 2559

[4] Chart.js.[ออนไลน์]. แหล่งที่มา: <http://www.chartjs.org/>

15 กรกฎาคม 2559

[5] OID Tree. [ออนไลน์]. แหล่งที่มา:

[http://ipmsupport.solarwinds.com/mibs\_byoidtree.asp](http://ipmsupport.solarwinds.com/mibs_byoidtree.aspx?oid=1.3.6.1.2.1.1.1#h)22 สิงหาคม 2559

[6] PHP. [ออนไลน์]. แหล่งที่มา:

<http://php.net/>

22 กรกฎาคม 2559

[7] PHP CURL POST & GET. [ออนไลน์].แหล่งที่มา: <http://hayageek.com/php-curl-post-get/>

11 สิงหาคม 2559

[8] SNMP. [ออนไลน์]. แหล่งที่มา:

https://th.wikipedia.org/wiki/

30 สิงหาคม 2559

[9] SNMP v1**.** [ออนไลน์]. แหล่งที่มา:

<https://sites.google.com/site/snmphorus/snmpv1>

30 สิงหาคม 2559

[10] SNMP v2. [ออนไลน์]. แหล่งที่มา:

<https://sites.google.com/site/snmphorus/snmpv2>

30 สิงหาคม 2559

[11] SNMP v3. [ออนไลน์]. แหล่งที่มา:

<https://sites.google.com/site/snmphorus/snmpv3>

30 สิงหาคม 2559