

คู่มือการปฏิบัติงาน
หน่วยเครือข่ายคอมพิวเตอร์
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏเชียงราย

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏเชียงราย

งานเทคโนโลยีสารสนเทศ

ตุลาคม พ.ศ. 2569

สารบัญ

	หน้า
วัตถุประสงค์	1
คำจำกัดความ	1
หน้าที่ความรับผิดชอบ	2
ขั้นตอนการปฏิบัติงาน	3
งานเฝ้าระวังและบำรุงรักษาอุปกรณ์สลับสัญญาณ (Network Switch)	3
งานเฝ้าระวังและบำรุงรักษาอุปกรณ์ปล่อยสัญญาณไร้สาย (Wireless Network)	7
งานเฝ้าระวังและตรวจสอบสถานะการใช้งานเครือข่าย (ISP Monitoring)	12
งานเฝ้าระวังและบำรุงรักษาการใช้เครื่องแม่ข่าย (Server Fram)	15
ภาคผนวก	19
ภาคผนวก ก ขั้นตอนการติดตั้งโปรแกรม PuTTY	20

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏเชียงราย

1. วัตถุประสงค์

1. กำหนดแนวทางการปฏิบัติงานด้านเครือข่ายคอมพิวเตอร์ให้เป็นมาตรฐานเดียวกัน ทั้งการเฝ้าระวัง การตรวจสอบ การบำรุงรักษา และการแก้ไขปัญหา
2. ดูแลให้อุปกรณ์ Network Switch, Wireless Network, ระบบเชื่อมต่ออินเทอร์เน็ต และเครื่องแม่ข่ายมีความพร้อมใช้งานอย่างต่อเนื่อง มีประสิทธิภาพ และรองรับภารกิจของมหาวิทยาลัย
3. ป้องกันและลดผลกระทบจากเหตุขัดข้องของระบบเครือข่าย รวมถึงกำหนดขั้นตอนการตรวจสอบ วิเคราะห์ และแก้ไขปัญหาให้สามารถดำเนินการได้อย่างรวดเร็วและเป็นระบบ
4. ส่งเสริมการบำรุงรักษาเชิงป้องกัน เสริมสร้างความมั่นคงปลอดภัย และควบคุมการเข้าถึงอุปกรณ์เครือข่ายให้เหมาะสม เพื่อยืดอายุการใช้งานและลดความเสียหาย
5. จัดเก็บข้อมูลอุปกรณ์ การตั้งค่า การเปลี่ยนแปลง ประวัติการบำรุงรักษา และรายงานเหตุขัดข้อง เพื่อใช้ติดตามสถานะ ตรวจสอบย้อนหลัง และวางแผนปรับปรุงระบบ
6. ใช้เป็นคู่มืออ้างอิงสำหรับการถ่ายทอดความรู้ การฝึกอบรม และการปฏิบัติงานแทนกันของเจ้าหน้าที่หน่วยเครือข่ายคอมพิวเตอร์

2. คำจำกัดความ

1. ระบบเครือข่ายคอมพิวเตอร์ หมายถึง ระบบที่เชื่อมโยงอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบสารสนเทศ เพื่อแลกเปลี่ยนข้อมูลและให้บริการแก่ผู้ใช้งาน
2. Network Switch หมายถึง อุปกรณ์สลับสัญญาณที่ใช้เชื่อมต่ออุปกรณ์ภายในเครือข่าย และส่งต่อข้อมูลไปยังพอร์ตหรืออุปกรณ์ปลายทางที่เกี่ยวข้อง
3. Wireless Network หมายถึง เครือข่ายคอมพิวเตอร์ที่เชื่อมต่อและรับส่งข้อมูลผ่านคลื่นวิทยุโดยไม่ใช้สายสัญญาณ
4. Access Point หมายถึง อุปกรณ์ที่ให้บริการเชื่อมต่อเครือข่ายไร้สาย และเชื่อมโยงผู้ใช้งานไร้สายเข้าสู่เครือข่ายของหน่วยงาน
5. ISP Monitoring หมายถึง การเฝ้าระวังและตรวจสอบสถานะ ประสิทธิภาพ และความต่อเนื่องของวงจรสื่อสารหรือบริการอินเทอร์เน็ตจากผู้ให้บริการ
6. Monitoring หมายถึง ระบบหรือเครื่องมือที่ใช้ติดตามสถานะ ประสิทธิภาพ เหตุแจ้งเตือน และเหตุการณ์ของอุปกรณ์หรือระบบเครือข่าย
7. เครื่องแม่ข่าย (Server) หมายถึง เครื่องคอมพิวเตอร์หรือระบบที่ให้บริการข้อมูล โปรแกรม ฐานข้อมูล หรือบริการเครือข่ายแก่ผู้ใช้งานหรืออุปกรณ์อื่น
8. Configuration หมายถึง ค่าการตั้งค่าของอุปกรณ์หรือระบบที่กำหนดให้ทำงานตามวัตถุประสงค์ เช่น การกำหนดพอร์ต VLAN สิทธิ์การเข้าถึง และเส้นทางเครือข่าย

9. Bandwidth หมายถึง ความสามารถสูงสุดในการรับส่งข้อมูลของช่องสัญญาณหรือวงจรสื่อสารในช่วงเวลาหนึ่ง
10. Latency หมายถึง ระยะเวลาที่ข้อมูลใช้ในการเดินทางจากต้นทางไปยังปลายทาง
11. Packet Loss หมายถึง การสูญหายของแพ็กเก็ตข้อมูลระหว่างการรับส่ง ซึ่งอาจส่งผลให้การสื่อสารล่าช้าหรือขาดช่วง
12. เหตุขัดข้อง หมายถึง เหตุการณ์ที่ทำให้อุปกรณ์ ระบบเครือข่าย หรือบริการไม่สามารถทำงานได้ตามปกติ หรือมีประสิทธิภาพลดลง
13. การบำรุงรักษาเชิงป้องกัน หมายถึง การตรวจสอบ ทำความสะอาด สำรองข้อมูล และปรับปรุงอุปกรณ์หรือระบบตามรอบเวลา เพื่อป้องกันการขัดข้องและยืดอายุการใช้งาน
14. Log หมายถึง บันทึกเหตุการณ์ การทำงาน หรือการเข้าใช้งานของอุปกรณ์และระบบ ซึ่งใช้สำหรับตรวจสอบและวิเคราะห์ปัญหา
15. ผู้รับผิดชอบ หมายถึง บุคลากรหรือหน่วยงานที่ได้รับมอบหมายให้ดูแล ตรวจสอบ บำรุงรักษา และประสานงานเกี่ยวกับอุปกรณ์หรือระบบตามคู่มือนี้

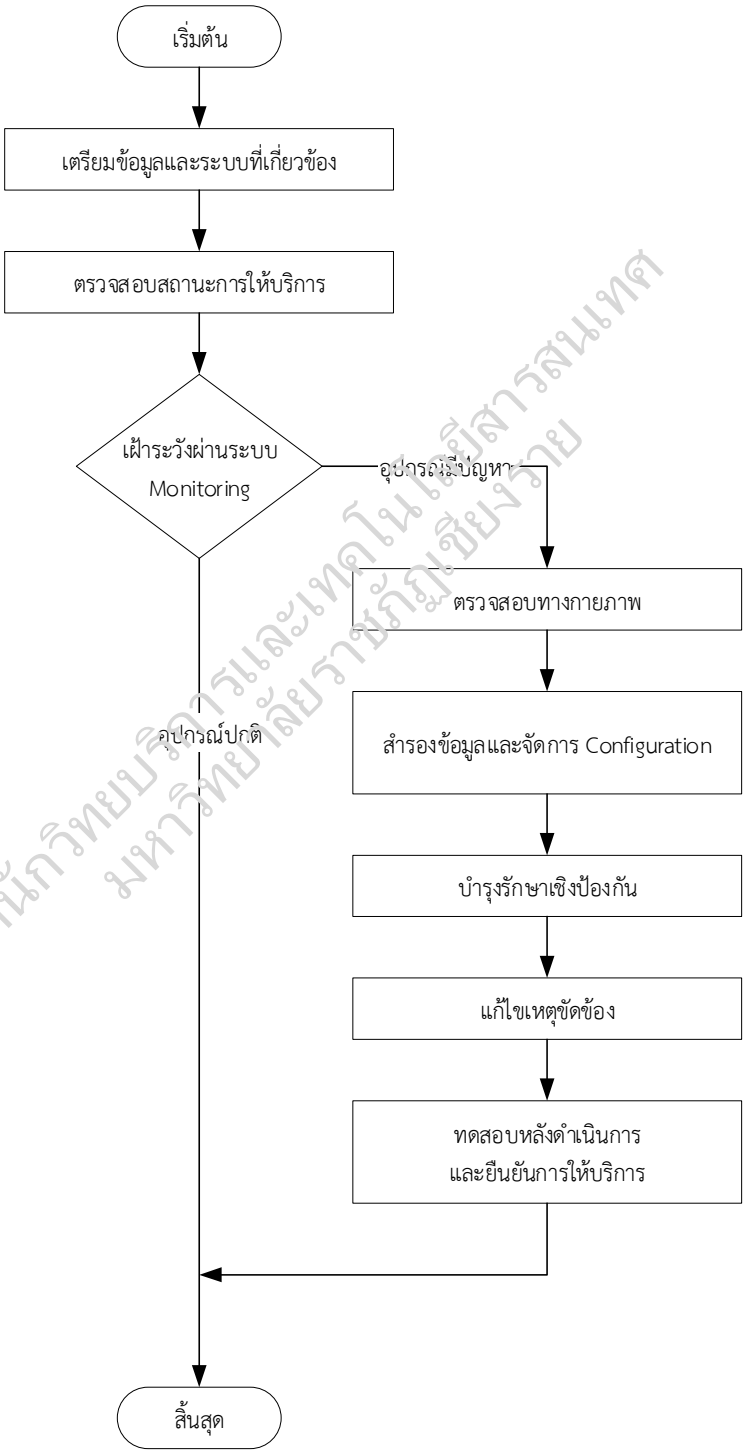
3. หน้าที่ความรับผิดชอบ

1. งานเฝ้าระวังและบำรุงรักษาอุปกรณ์สลับสัญญาณ (Network Switch) มีหน้าที่ตรวจสอบสถานะการทำงานของอุปกรณ์ พอร์ตเชื่อมต่อ สายสัญญาณ อุณหภูมิ การใช้ทรัพยากร และเหตุการณ์ผิดปกติ สำรองและควบคุมการตั้งค่า ดำเนินการบำรุงรักษาเชิงป้องกัน แก้ไขเหตุขัดข้อง และทดสอบการให้บริการหลังดำเนินการ
2. งานเฝ้าระวังและบำรุงรักษาอุปกรณ์ปล่อยสัญญาณไร้สาย (Wireless Network) มีหน้าที่ตรวจสอบสถานะ Access Point คุณภาพและความครอบคลุมของสัญญาณ จำนวนผู้ใช้งาน สัญญาณรบกวน ความมั่นคงปลอดภัย และการเชื่อมต่อกับระบบบริหารจัดการ รวมทั้งบำรุงรักษา แก้ไขปัญหา และทดสอบการให้บริการ Wi-Fi
3. งานเฝ้าระวังและตรวจสอบสถานะการใช้งานเครือข่าย (ISP Monitoring) มีหน้าที่ตรวจสอบสถานะวงจรอินเทอร์เน็ตและอุปกรณ์ที่เกี่ยวข้อง ติดตาม Bandwidth, Latency, Packet Loss และ Jitter ตรวจสอบเหตุแจ้งเตือน ประสานงานกับผู้ให้บริการ ติดตามการแก้ไข และยืนยันว่าบริการกลับมาใช้งานได้ตามปกติ
4. งานเฝ้าระวังและบำรุงรักษาเครื่องแม่ข่าย (Server) มีหน้าที่ตรวจสอบสถานะเครื่องแม่ข่าย บริการระบบ ฐานข้อมูล การใช้ CPU หน่วยความจำ พื้นที่จัดเก็บข้อมูล และความมั่นคงปลอดภัย สำรองข้อมูลและ Configuration แก้ไขเหตุขัดข้อง กู้คืนบริการ และทดสอบระบบหลังดำเนินการ

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏเชียงราย

4. ขั้นตอนการปฏิบัติงาน

4.1 งานเฝ้าระวังและบำรุงรักษาอุปกรณ์สลับสัญญาณ(Network Switch)

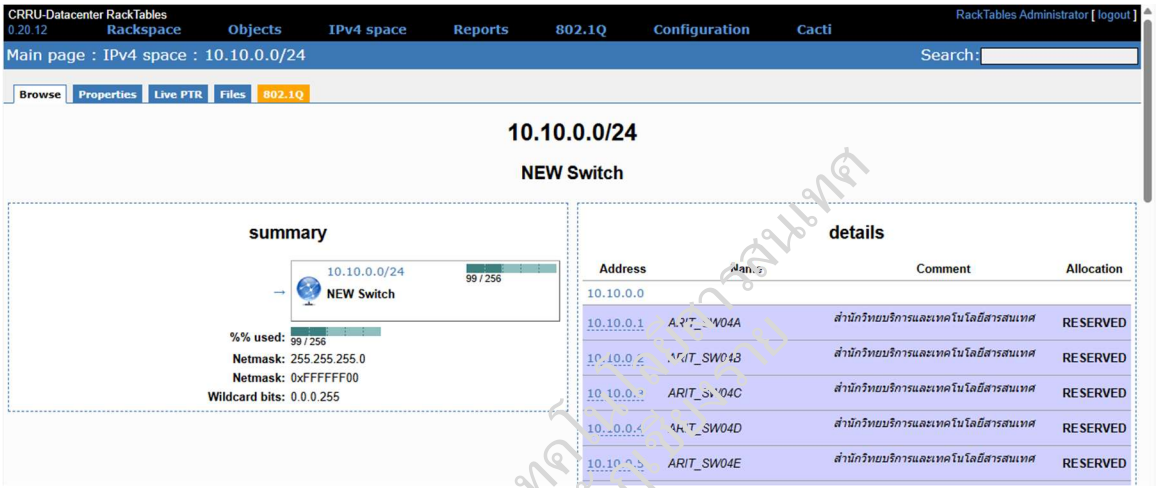


สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏเชียงราย

ขั้นตอนการปฏิบัติงานเฝ้าระวังและบำรุงรักษาอุปกรณ์สลับสัญญาณ (Network Switch)

1. เตรียมข้อมูลและระบบที่เกี่ยวข้อง

ตรวจสอบรายชื่อ ตำแหน่งติดตั้ง หมายเลข IP ชื่ออุปกรณ์ ผู้รับผิดชอบ ผังเครือข่าย คู่มือรุ่นอุปกรณ์ สิทธิ์การเข้าใช้งาน ผ่านเว็บไซต์ ip.crru.ac.th ดังรูป



รูปที่ 1 แสดงหน้าจอ หมายเลข IP ชื่ออุปกรณ์

2. ตรวจสอบสถานการณ์ให้บริการ

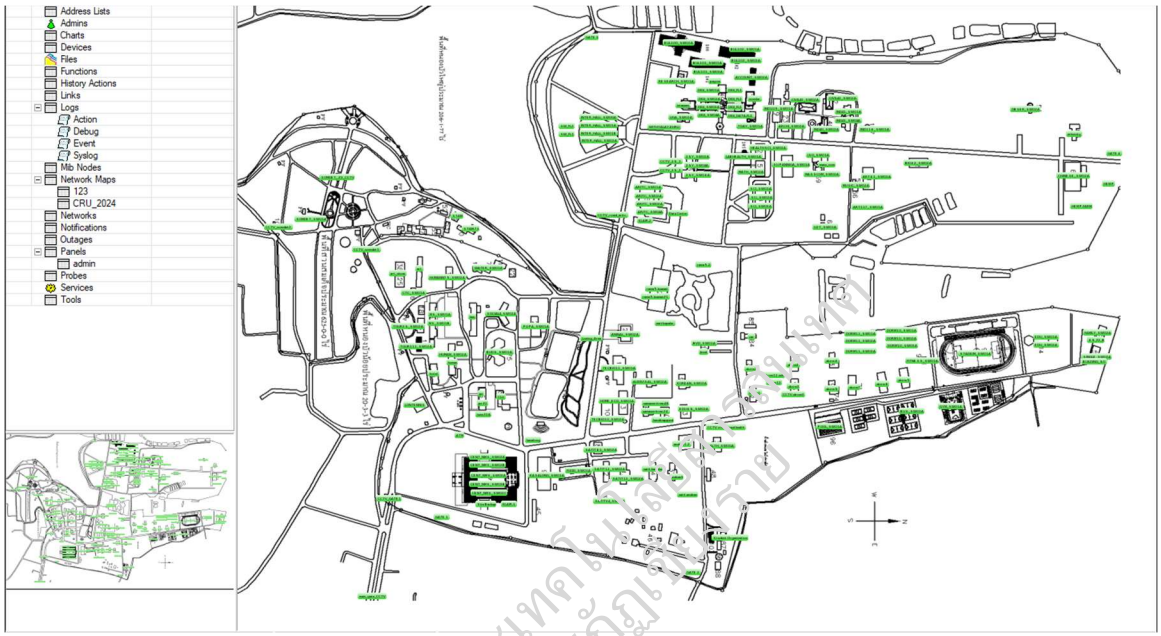
ตรวจสอบการทำงานของ Switch สถานะไฟ Power, Link, SFP และ Alarm อุณหภูมิ การใช้ CPU หน่วยความจำ สถานะพอร์ต อุปกรณ์ที่เชื่อมต่อ และเหตุการณ์ผิดปกติ โดยเชื่อมอุปกรณ์ผ่านซอฟต์แวร์ SSH เช่น putty หรือ Termius เป็นต้น ดังรูป



รูปที่ 2 แสดงหน้าจอ การเชื่อมต่ออุปกรณ์

3. เฝ้าระวังผ่านระบบ Monitoring

ตรวจสอบ Dashboard แจ้งเตือนของอุปกรณ์ โดยใช้งานผ่านซอฟต์แวร์ The Dude ดังรูป



รูปที่ 3 แสดงหน้าจอ Dashboard แจ้งเตือนของอุปกรณ์

4. ตรวจสอบทางกายภาพ

ตรวจสอบตู้ Rack การยึดอุปกรณ์ สายไฟ สาย LAN สาย Fiber หัวเชื่อมต่อ ฝุ่น ความชื้น ระบบระบายความร้อน UPS และระบบไฟฟ้าสำรอง โดยห้ามถอดสายหรือปิดอุปกรณ์โดยไม่ได้รับอนุมัติ

5. สำรองข้อมูลและจัดการ Configuration

สำรองไฟล์ Configuration ก่อนและหลังการเปลี่ยนแปลง ตรวจสอบเวลาอุปกรณ์และ NTP บัญชีผู้ใช้งาน สิทธิ์การเข้าถึง Firmware หรือ Software Version และบันทึกประวัติการเปลี่ยนแปลง

6. บำรุงรักษาเชิงป้องกัน

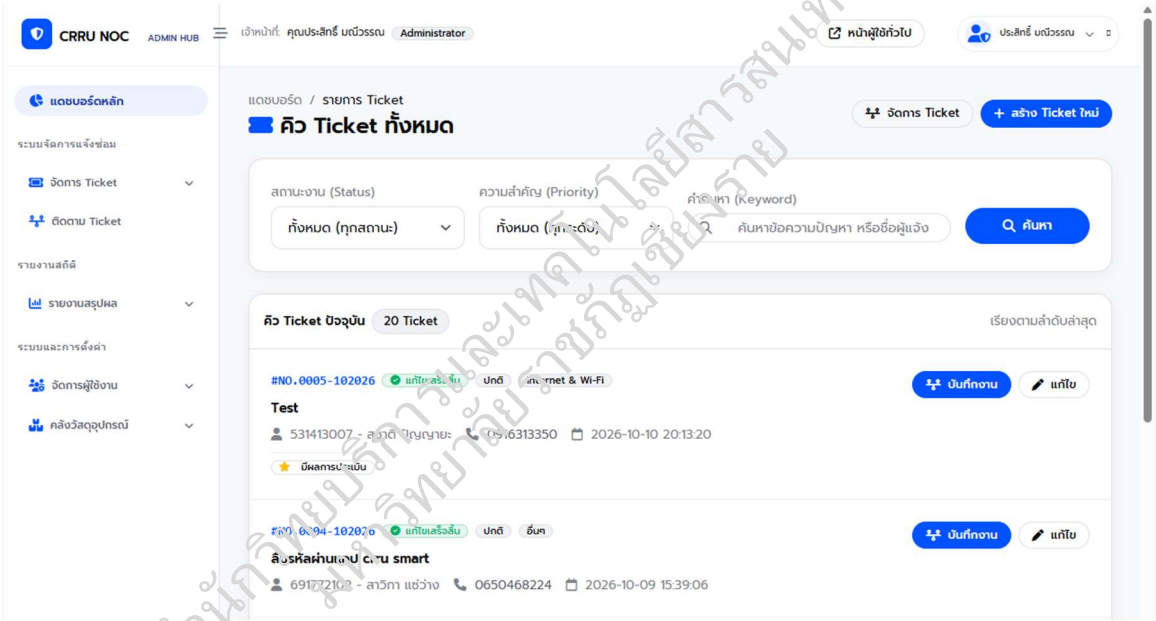
ทำความสะอาดอุปกรณ์และตู้ Rack จัดระเบียบสายสัญญาณ ตรวจสอบป้ายชื่อและหมายเลขพอร์ต ทดสอบไฟฟ้าสำรอง ปิดพอร์ตที่ไม่ได้ใช้งานเมื่อเหมาะสม และทบทวนการตั้งค่า VLAN, Trunk, STP และ Port Security

7. แก้ไขเหตุขัดข้อง

รับแจ้งและบันทึกปัญหา วิเคราะห์สาเหตุจากอุปกรณ์ สายสัญญาณ ไฟฟ้า หรือระบบเครือข่าย ตรวจสอบพอร์ตและ Log ทดสอบสายหรือเปลี่ยนพอร์ต ดำเนินการ Restart หรือเปลี่ยนอุปกรณ์เมื่อได้รับอนุมัติ และประสานผู้เชี่ยวชาญเมื่อจำเป็น

8. ทดสอบหลังดำเนินการและยืนยันการให้บริการ

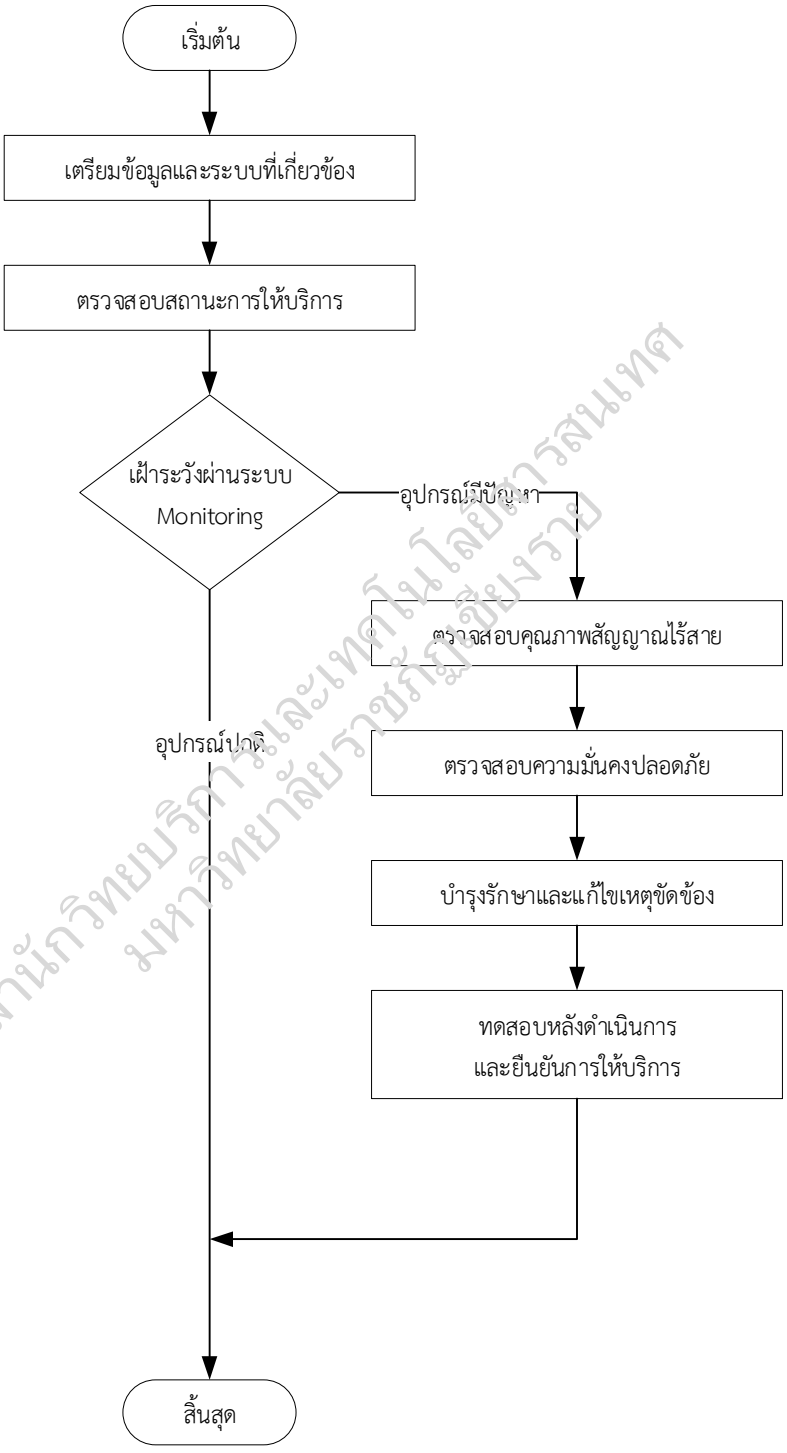
ทดสอบการเชื่อมต่อระหว่างอุปกรณ์ การรับ–ส่งข้อมูล VLAN และเส้นทางเครือข่าย ตรวจสอบค่าแจ้งเตือนให้กลับสู่สถานะปกติ และยืนยันว่าผู้ใช้งานสามารถใช้งานระบบได้ตามปกติ ซึ่งสามารถดำเนินการในระบบแจ้งซ่อมและติดตาม Ticket เครือข่าย (noc.crru.ac.th) ดังรูป



รูปที่ 4 แสดงหน้าจอ ระบบแจ้งซ่อมและติดตาม Ticket เครือข่าย

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏเชียงราย

4.2 งานเฝ้าระวังและบำรุงรักษาอุปกรณ์ปล่อยสัญญาณไร้สาย (Wireless Network)



สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสงขลา

ขั้นตอนการปฏิบัติงานเฝ้าระวังและบำรุงรักษาอุปกรณ์ปล่อยสัญญาณไร้สาย (Wireless Network)

1. เตรียมข้อมูลและระบบที่เกี่ยวข้อง

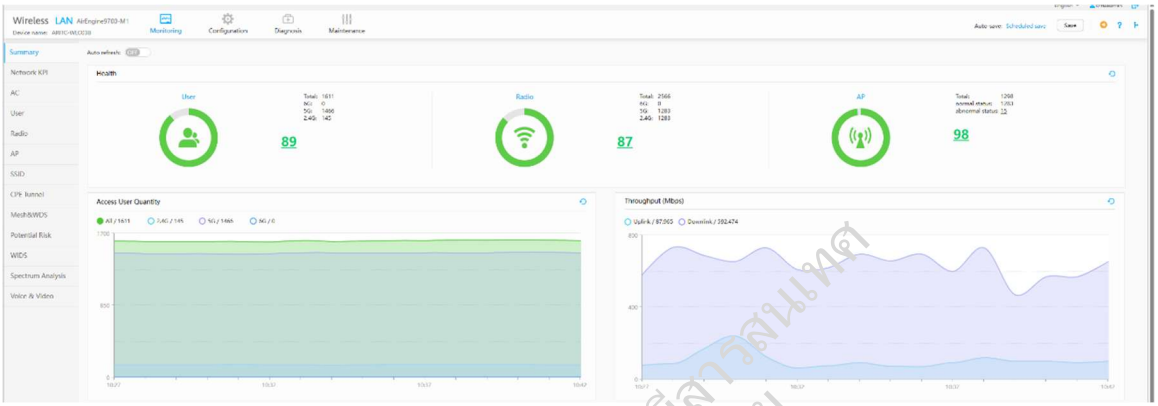
ตรวจสอบรายชื่อ ตำแหน่งติดตั้ง หมายเลขอุปกรณ์ ผู้รับผิดชอบ Access Point แผนผังเครือข่าย และระบบบริหารจัดการ Wireless ซึ่งจัดเก็บข้อมูลในรูปแบบไฟล์ .xlsx (Excel) ดังรูป

	จุดติดตั้งอุปกรณ์สลับสัญญาณ 10 Gbps. และ อุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (ระยะที่ 1)				
2	ลำดับ	ชื่ออาคาร	ชื่ออุปกรณ์	หมายเลข IP Address	ตำแหน่งติดตั้ง
3	1	1.คณะมนุษย์ศาสตร์	HUMAN_AP01A	10.10.8.11	ห้องฝ่ายเจ้าหน้าที่
4	2	1.คณะมนุษย์ศาสตร์	HUMAN_AP01B	10.10.8.12	ห้องสำนักงานคณบดี
5	3	1.คณะมนุษย์ศาสตร์	HUMAN_AP01C	10.10.8.13	ห้องสมุด
6	4	1.คณะมนุษย์ศาสตร์	HUMAN_AP01D	10.10.8.14	ห้องพักอาจารย์
7	5	1.คณะมนุษย์ศาสตร์	HUMAN_AP01E	10.10.8.15	ห้องพักอาจารย์
8	6	1.คณะมนุษย์ศาสตร์	HUMAN_AP01F	10.10.8.16	ลานเอนกประสงค์
9	7	1.คณะมนุษย์ศาสตร์	HUMAN_AP01G	10.10.8.17	โถงถางเดินหน้าบันได
10	8	1.คณะมนุษย์ศาสตร์	HUMAN_AP01H	10.10.8.18	โถงถางเดินหน้าบันได
11	9	1.คณะมนุษย์ศาสตร์	HUMAN_AP02A	10.10.8.19	ห้องเรียน
12	10	1.คณะมนุษย์ศาสตร์	HUMAN_AP02B	10.10.8.20	ห้องเรียน
13	11	1.คณะมนุษย์ศาสตร์	HUMAN_AP02C	10.10.8.21	ห้องประชุม
14	12	1.คณะมนุษย์ศาสตร์	HUMAN_AP03A	10.10.8.22	ห้องเรียน
15	13	1.คณะมนุษย์ศาสตร์	HUMAN_AP03B	10.10.8.23	ห้องเรียน
16	14	1.คณะมนุษย์ศาสตร์	HUMAN_AP03C	10.10.8.24	ห้องเรียน
17	15	1.คณะมนุษย์ศาสตร์	HUMAN_AP03D	10.10.8.25	ห้องเรียน
18	16	114.คณะครุศาสตร์	EDU_AP0GA	10.10.8.26	โถงถางเดินข้างสำนักงาน
19	17	114.คณะครุศาสตร์	EDU_AP0GB	10.10.8.27	สำนักงาน
20	18	114.คณะครุศาสตร์	EDU_AP01A	10.10.8.28	ห้องสารสนเทศ
21	19	114.คณะครุศาสตร์	EDU_AP01B	10.10.8.29	ห้องเรียน
22	20	114.คณะครุศาสตร์	EDU_AP01C	10.10.8.30	ห้องเรียน
23	21	114.คณะครุศาสตร์	EDU_AP01D	10.10.8.31	หน้าห้องคณบดี
24	22	114.คณะครุศาสตร์	EDU_AP01E	10.10.8.32	หน้าห้องประชุม
25	23	114.คณะครุศาสตร์	EDU_AP01F	10.10.8.33	ห้องเรียน
26	24	114.คณะครุศาสตร์	EDU_AP01G	10.10.8.34	ห้องเรียนรวมสโลป
27	25	114.คณะครุศาสตร์	EDU_AP01H	10.10.8.35	ห้องเรียนรวมสโลป
28	26	114.คณะครุศาสตร์	EDU_AP01I	10.10.8.36	ห้องเรียนรวม
29	27	114.คณะครุศาสตร์	EDU_AP02A	10.10.8.37	ห้องคอมพิวเตอร์

รูปที่ 5 แสดงหน้าจอ รายชื่อ ตำแหน่งติดตั้ง และหมายเลขอุปกรณ์

2. ตรวจสอบสถานการณ์ให้บริการ

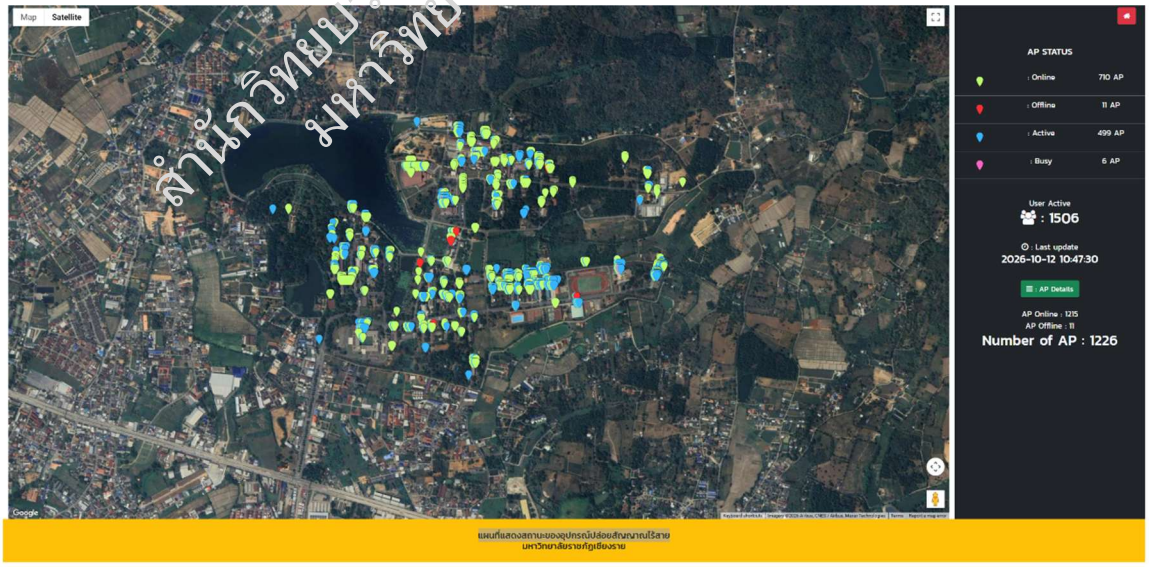
ตรวจสอบสถานะ Access Point การเชื่อมต่อกับระบบบริหารจัดการ สถานะไฟฟ้า พอร์ต เครือข่าย จำนวนผู้ใช้งาน และสัญญาณแจ้งเตือน ผ่านระบบ WiFi Controller ดังรูป



รูปที่ 6 แสดงหน้าจอ ตรวจสอบสถานะ Access Point

3. เฝ้าระวังผ่านระบบ Monitoring

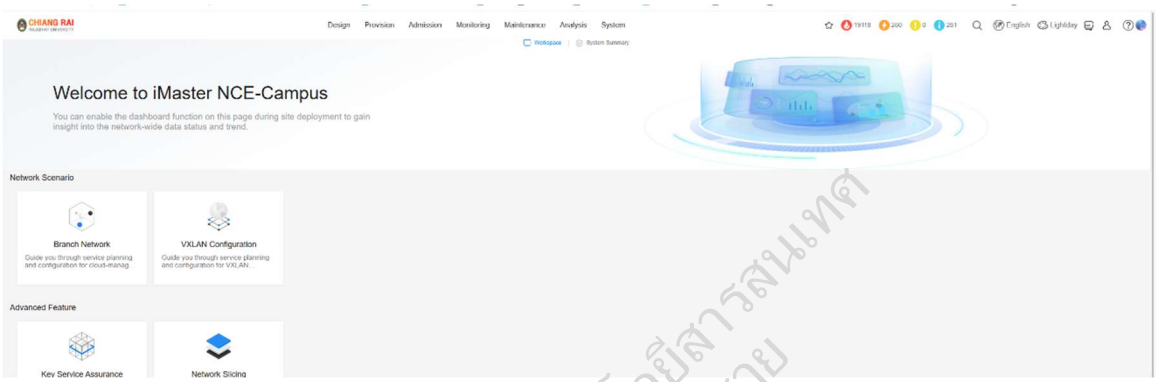
ตรวจสอบ Dashboard ของระบบ Monitoring ที่ใช้ติดตามสถานะอุปกรณ์เครือข่ายและการให้บริการ ได้แก่ สถานะการทำงานของอุปกรณ์ หรือเหตุการณ์ผิดปกติ ผ่านระบบแผนที่แสดงสถานะของอุปกรณ์ปล่อยสัญญาณไร้สาย (apmap.cnn.ac.th) ดังรูป



รูปที่ 7 แสดงหน้าจอ ตรวจสอบ Dashboard ของระบบ Monitoring

4. ตรวจสอบคุณภาพสัญญาณไร้สาย

ตรวจสอบระดับความแรงของสัญญาณ พื้นที่อับสัญญาณ สัญญาณรบกวน ความเร็ว และความครอบคลุมของพื้นที่ให้บริการ สามารถดำเนินการผ่านระบบจัดการและควบคุมเครือข่ายอัจฉริยะ (iMaster NCE-Campus) ดังรูป



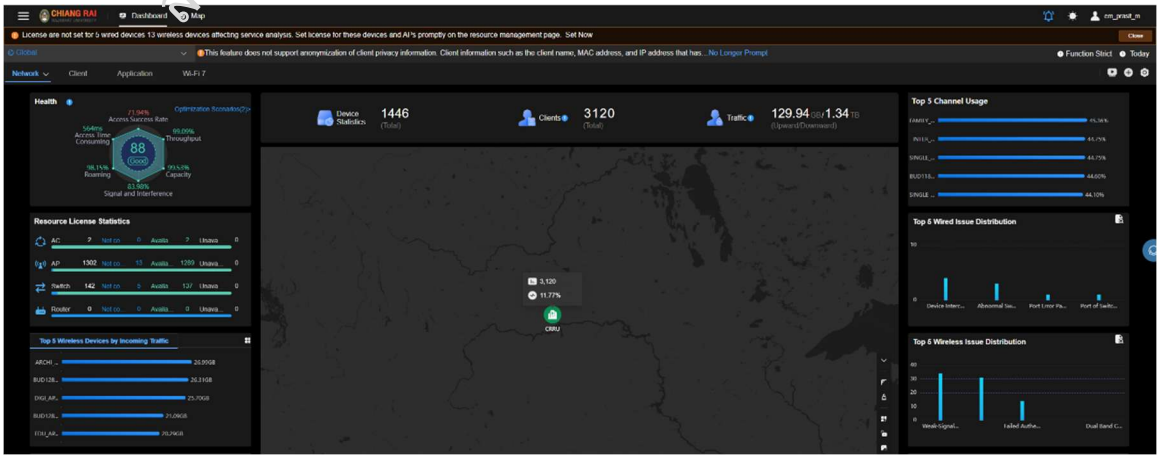
รูปที่ 8 แสดงหน้าจอ ตรวจสอบระดับความแรงของสัญญาณ

5. ตรวจสอบความมั่นคงปลอดภัย

ตรวจสอบชื่อเครือข่าย รูปแบบการเข้ารหัส สิทธิ์การเข้าถึง อุปกรณ์ที่เชื่อมต่อ บัญชีผู้ดูแลระบบ และ Log การใช้งาน

6. บำรุงรักษาและแก้ไขเหตุขัดข้อง

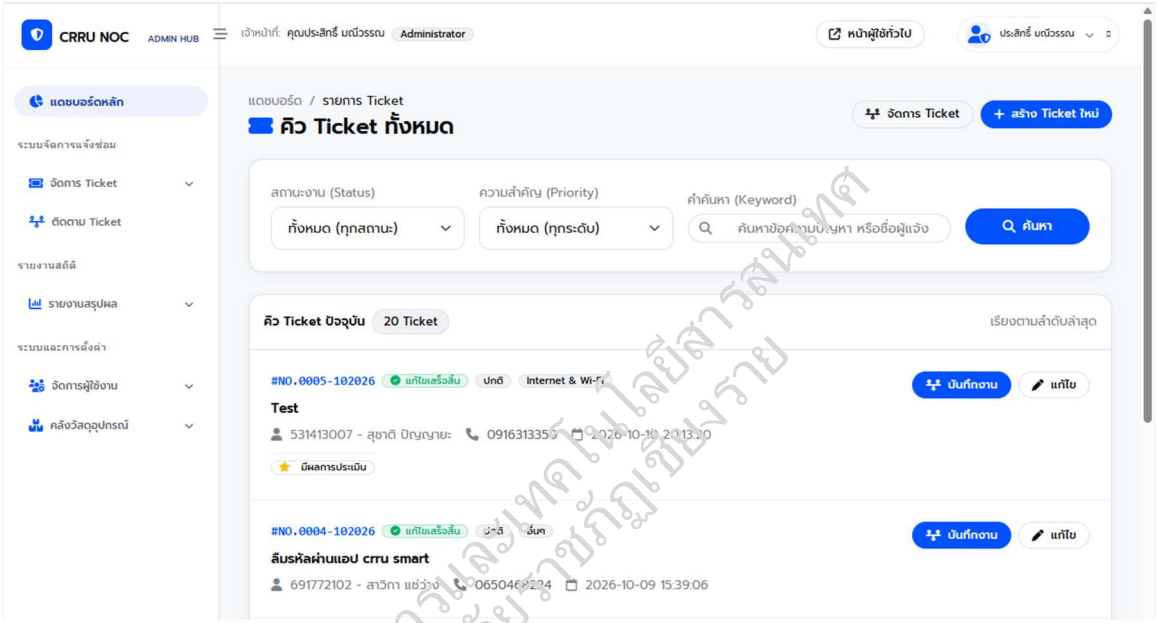
ตรวจสอบสภาพอุปกรณ์ สายสัญญาณ อุปกรณ์จ่ายไฟ Firmware และสำรองข้อมูลการตั้งค่า รวมถึงวิเคราะห์และแก้ไขปัญหาเบื้องต้น สามารถดำเนินการผ่านระบบวิเคราะห์เครือข่ายอัจฉริยะ (iMaster NCE-CampusInsight) ดังรูป



รูปที่ 9 แสดงหน้าจอ ตรวจสอบสภาพอุปกรณ์

7. ทดสอบหลังดำเนินการและยืนยันการให้บริการ

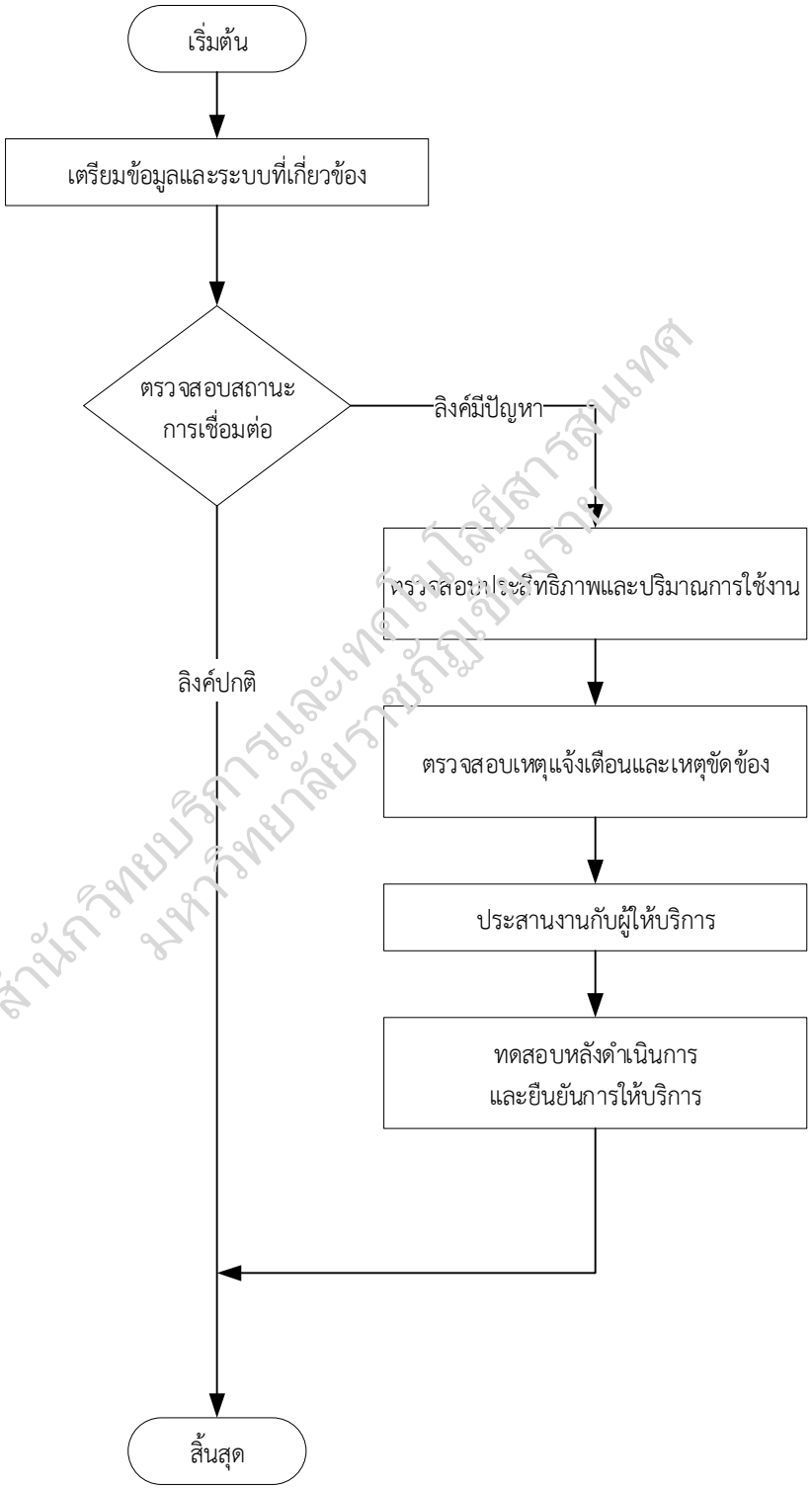
ทดสอบการเชื่อมต่อ Wi-Fi การรับ–ส่งข้อมูล ความเร็ว และตรวจสอบสถานะ Access Point ในระบบ Monitoring ก่อนแจ้งผู้เกี่ยวข้อง ซึ่งสามารถดำเนินการในระบบแจ้งซ่อมและติดตาม Ticket เครือข่าย (noc.crru.ac.th) ดังรูป



รูปที่ 10 แสดงหน้าจอ ระบบแจ้งซ่อมและติดตาม Ticket เครือข่าย

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏเชียงราย

4.3 งานเฝ้าระวังและตรวจสอบสถานะการใช้งานเครือข่าย (ISP Monitoring)



สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏเชียงราย

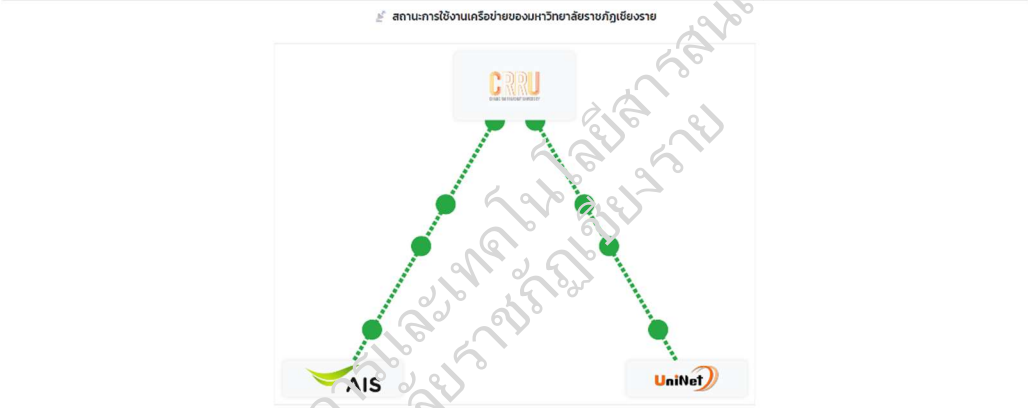
ขั้นตอนการปฏิบัติงานเฝ้าระวังและตรวจสอบสถานะการใช้งานเครือข่าย (ISP Monitoring)

1. เตรียมข้อมูลและระบบที่เกี่ยวข้อง

   ตรวจสอบข้อมูลผู้ให้บริการ สัญญา SLA ระบบ Monitoring และผู้รับผิดชอบ

2. ตรวจสอบสถานการณ์เชื่อมต่อ

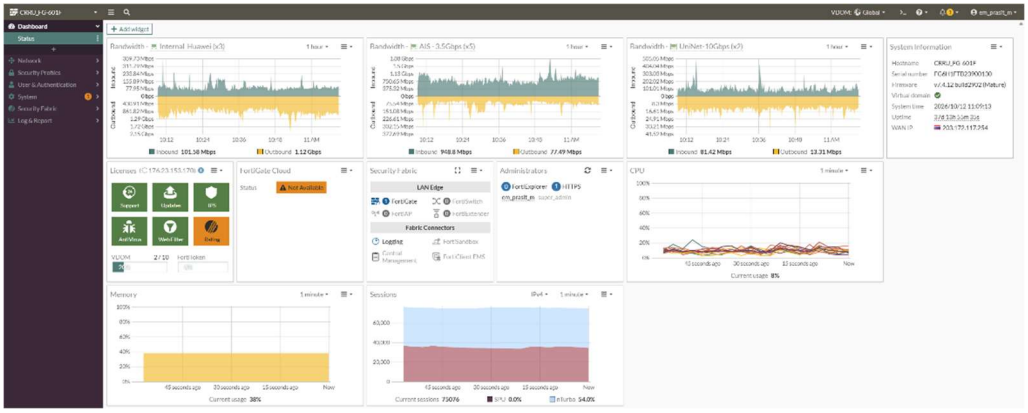
   ตรวจสอบสถานะวงจรอินเทอร์เน็ต Link, Interface, Router, Firewall และการเข้าถึงระบบงานสำคัญ ผ่านระบบสถานการณ์ใช้งานเครือข่ายของมหาวิทยาลัย (apmap.crru.ac.th/port) ดังรูป



รูปที่ 11 แสดงหน้าจอ สถานะวงจรอินเทอร์เน็ต

3. ตรวจสอบประสิทธิภาพและปริมาณการใช้งาน

   ตรวจสอบ Bandwidth, Latency, Packet Loss, Jitter และแนวโน้มการใช้งานเครือข่าย ผ่านระบบรักษาความปลอดภัยเครือข่าย ดังรูป



รูปที่ 12 แสดงหน้าจอ ตรวจสอบ Bandwidth

4. ตรวจสอบเหตุแจ้งเตือนและเหตุขัดข้อง

   ตรวจสอบ Alarm, Log ระยะเวลาที่ขัดข้อง พื้นที่ได้รับผลกระทบ และวิเคราะห์สาเหตุเบื้องต้น

5. ประสานงานกับผู้ให้บริการ

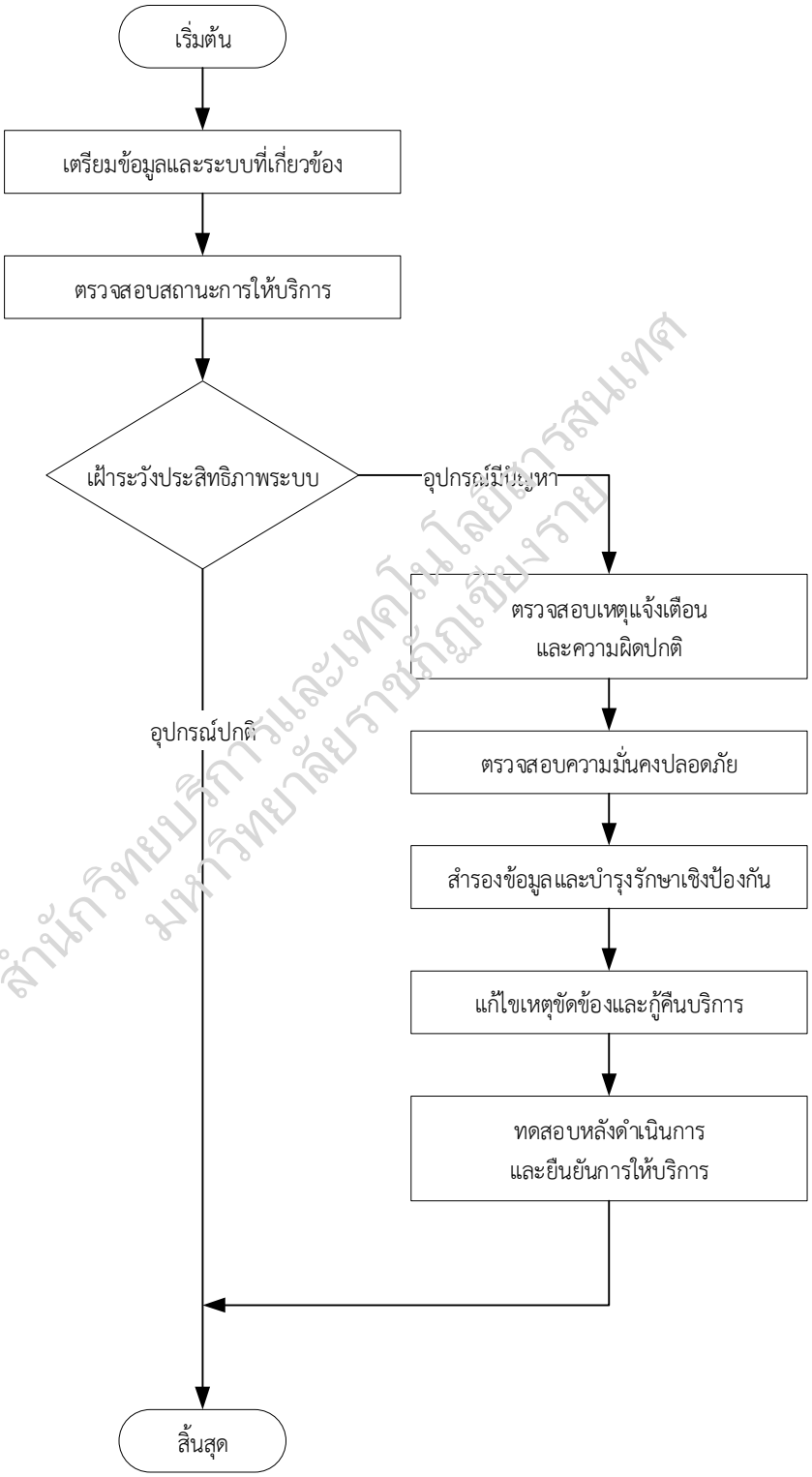
   แจ้งเหตุขัดข้อง ระบุข้อมูลวงจร ติดตามหมายเลขงานและความคืบหน้า จนกว่าระบบจะกลับเป็นปกติ

6. ทดสอบหลังแก้ไขและยืนยันการให้บริการ

   ทดสอบการเชื่อมต่อ ความเร็ว Latency, Packet Loss และยืนยันว่าผู้ใช้งานสามารถใช้บริการได้ตามปกติ

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏเชียงราย

4.4 งานเฝ้าระวังและบำรุงรักษาการใช้เครื่องแม่ข่าย (Server Fram)

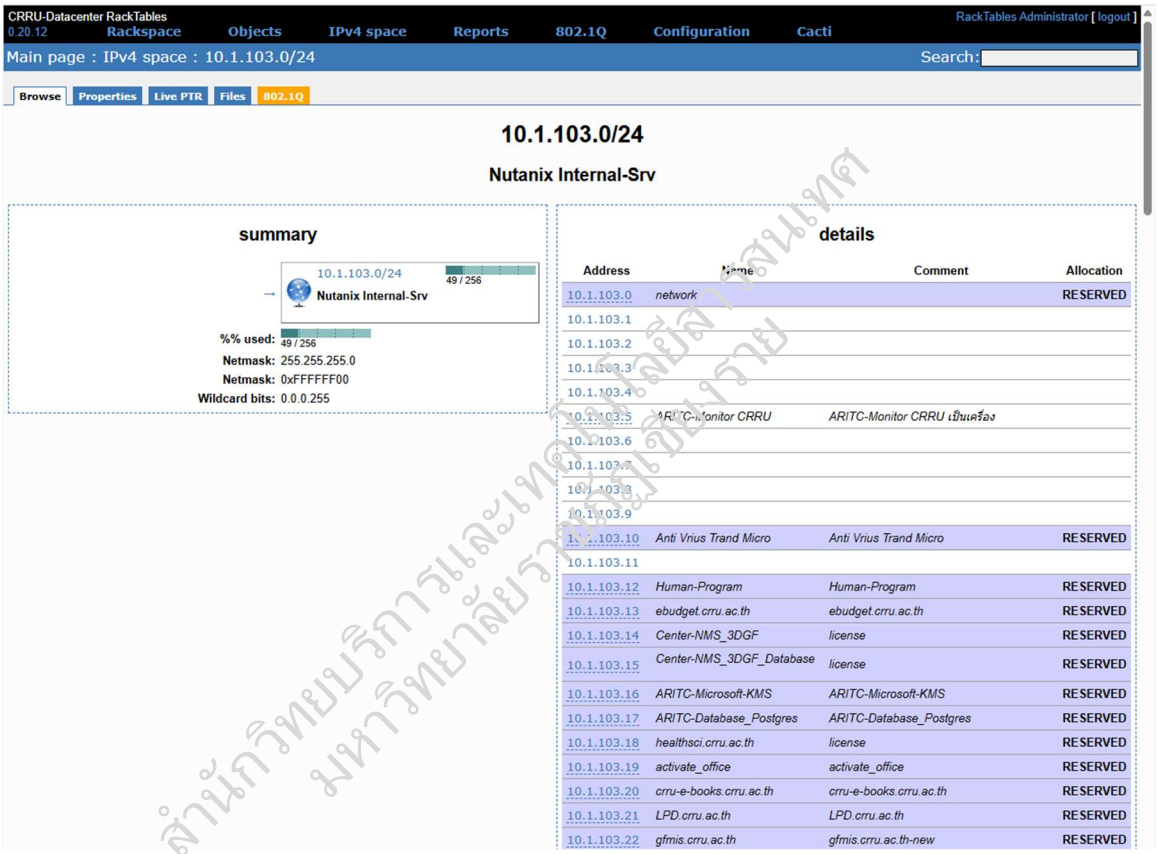


สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏเชียงราย

ขั้นตอนการปฏิบัติงานเฝ้าระวังและบำรุงรักษาการใช้เครื่องแม่ข่าย (Server Fram)

1. เตรียมข้อมูลและระบบที่เกี่ยวข้อง

ตรวจสอบรายชื่อเครื่องแม่ข่าย หมายเลข IP ชื่อเครื่อง ตำแหน่งติดตั้ง ระบบปฏิบัติการ บริการที่ให้บริการ ผู้รับผิดชอบ และสิทธิ์การเข้าใช้งาน ผ่านเว็บไซต์ ip.crru.ac.th ดังรูป



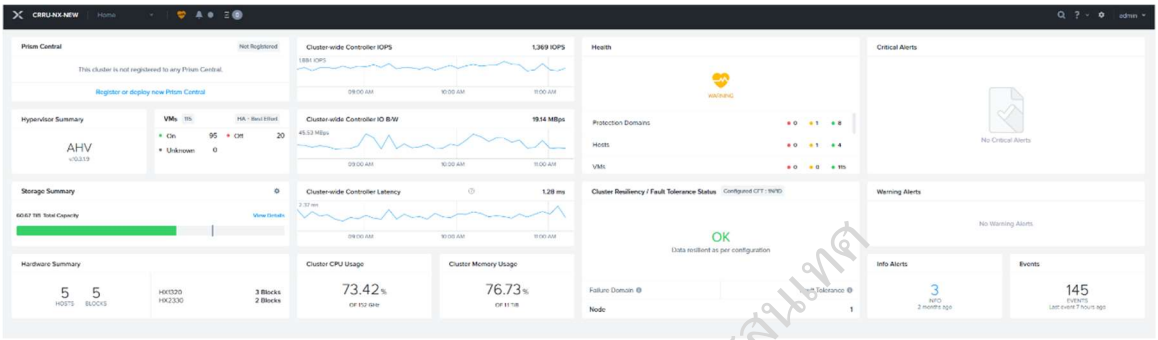
รูปที่ 13 แสดงหน้าจอ รายชื่อเครื่องแม่ข่าย หมายเลข IP ชื่อเครื่อง

2. ตรวจสอบสถานการณ์ให้บริการ

ตรวจสอบสถานะการทำงานของเครื่องแม่ข่าย การเปิดใช้งานระบบ บริการสำคัญ การเชื่อมต่อเครือข่าย และการเข้าถึงจากผู้ใช้งาน

3. เฝ้าระวังประสิทธิภาพระบบ

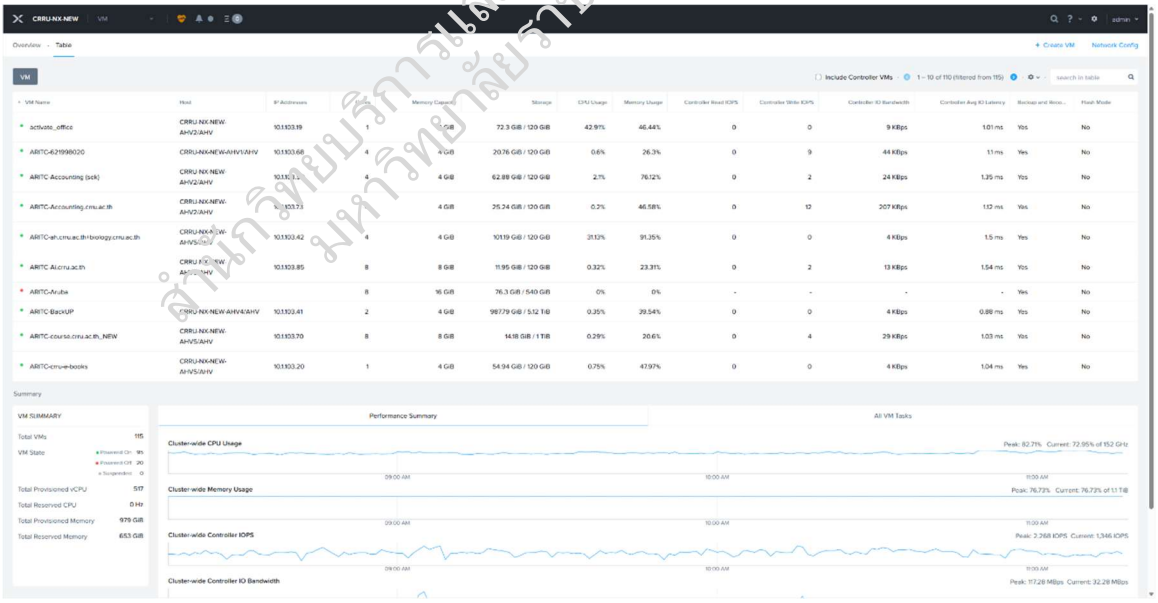
ตรวจสอบการใช้ CPU หน่วยความจำ พื้นที่จัดเก็บข้อมูล อุณหภูมิ ปริมาณการรับ–ส่งข้อมูล และทรัพยากรของระบบผ่านเครื่องมือ Monitoring ดังรูป



รูปที่ 14 แสดงหน้าจอ ตรวจสอบการใช้ CPU หน่วยความจำ พื้นที่จัดเก็บข้อมูล

4. ตรวจสอบเหตุแจ้งเตือนและความผิดปกติ

ตรวจสอบ Alarm, Event Log และ System Log วิเคราะห์ข้อผิดพลาด การหยุดทำงานของบริการ การใช้ทรัพยากรสูง และเหตุการณ์ที่อาจส่งผลกระทบต่อระบบ ดังรูป



รูปที่ 15 แสดงหน้าจอ ตรวจสอบ Alarm, Event Log และ System Log

5. ตรวจสอบความมั่นคงปลอดภัย

ตรวจสอบบัญชีผู้ใช้งาน สิทธิ์การเข้าถึง การเข้าสู่ระบบที่ผิดปกติ การอัปเดตระบบปฏิบัติการ โปรแกรมป้องกันมัลแวร์ และการตั้งค่าความปลอดภัย

6. สำรองข้อมูลและบำรุงรักษาเชิงป้องกัน

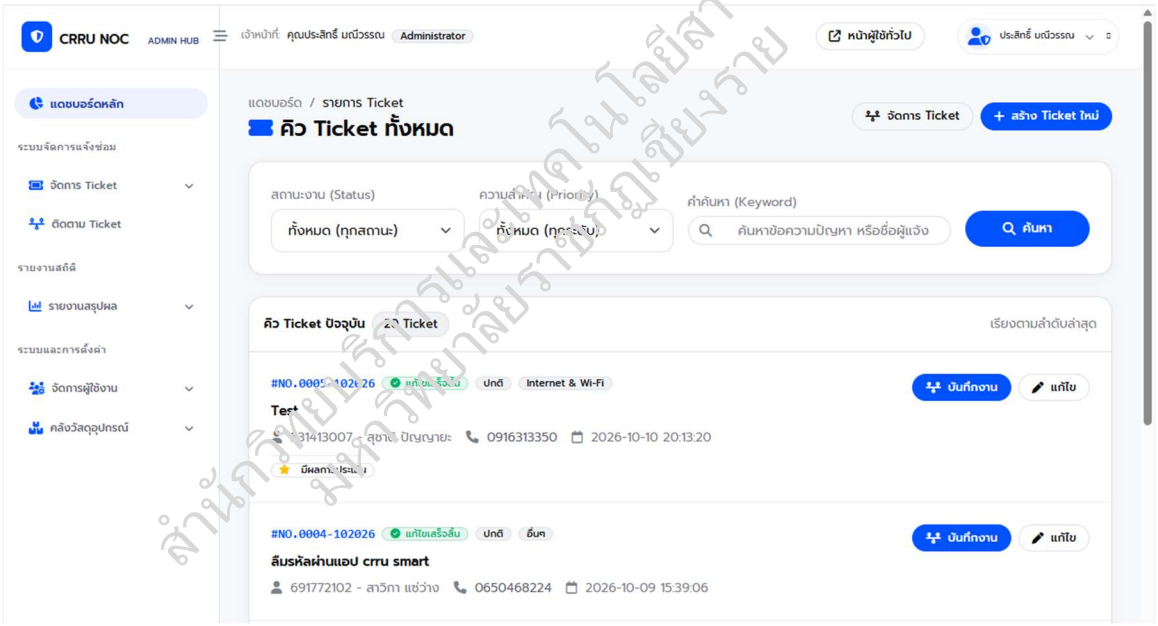
สำรองข้อมูลระบบ ฐานข้อมูล และ Configuration ตามรอบเวลา ตรวจสอบผลการสำรองข้อมูล ทำความสะอาดอุปกรณ์ ตรวจสอบพื้นที่จัดเก็บ และทดสอบระบบไฟฟ้าสำรอง

7. แก้ไขเหตุขัดข้องและกู้คืนบริการ

รับแจ้งและบันทึกปัญหา วิเคราะห์สาเหตุจากฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่าย หรือฐานข้อมูล ดำเนินการแก้ไขและกู้คืนบริการตามลำดับความสำคัญ พร้อมประสานผู้เชี่ยวชาญเมื่อจำเป็น

8. ทดสอบหลังดำเนินการและยืนยันการให้บริการ

ทดสอบการทำงานของเครื่องแม่ข่าย บริการ ระบบฐานข้อมูล การเชื่อมต่อเครือข่าย และการเข้าถึงของผู้ใช้งาน ตรวจสอบค่าแจ้งเตือนให้กลับสู่สถานะปกติ ซึ่งสามารถดำเนินการในระบบแจ้งซ่อมและติดตาม Ticket เครือข่าย (noc.crru.ac.th) ดังรูป



รูปที่ 16 แสดงหน้าจอ ระบบแจ้งซ่อมและติดตาม Ticket เครือข่าย

ภาคผนวก

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏเชียงราย

ภาคผนวก ก

ขั้นตอนการติดตั้งโปรแกรม PuTTY

PuTTY เป็นโปรแกรมฟรีสำหรับเชื่อมต่อไปยังเครื่องเซิร์ฟเวอร์ระยะไกลผ่าน SSH, Telnet และพอร์ต Serial เอกสารนี้อธิบายขั้นตอนการติดตั้ง PuTTY บน Windows ตั้งแต่ดาวน์โหลดไฟล์จนถึงทดสอบการเชื่อมต่อครั้งแรก

สิ่งที่ต้องเตรียม

- เครื่องคอมพิวเตอร์ที่ใช้ Windows 10 หรือ Windows 11
- สิทธิ์ผู้ดูแลระบบ (Administrator) ของเครื่อง สำหรับยืนยันการติดตั้ง
- การเชื่อมต่ออินเทอร์เน็ต และ IP Address หรือชื่อเครื่องของเซิร์ฟเวอร์ที่ต้องการเชื่อมต่อ

หมายเหตุ: รูปภาพในเอกสารนี้เป็นภาพจำลองหน้าจอเพื่อประกอบคำอธิบาย หน้าจอจริงและหมายเลขเวอร์ชันอาจแตกต่างเล็กน้อย

ขั้นตอนที่ 1: ดาวน์โหลดไฟล์ติดตั้ง

เปิดเว็บเบราว์เซอร์แล้วไปที่เว็บไซต์ทางการของ PuTTY ที่ https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
จากนั้นคลิกลิงก์ไปยังหน้าดาวน์โหลด ในหัวข้อ MSI (‘Windows Installer’) ให้เลือกไฟล์ที่ตรงกับเครื่อง โดยเครื่องส่วนใหญ่ในปัจจุบันใช้ 64-bit x36

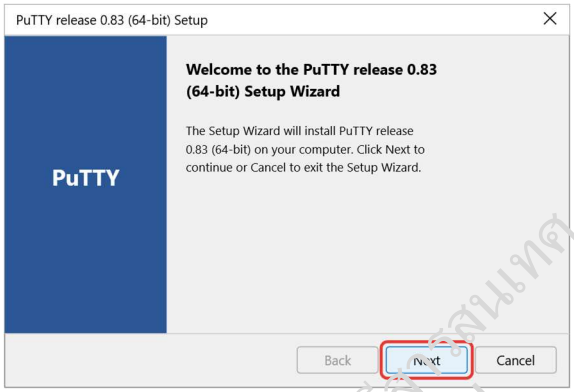
(ระวังอย่าดาวน์โหลดจากเว็บไซต์อื่นที่ไม่ใช่ของผู้พัฒนา เพราะอาจมีไฟล์ปลอมที่แฝงมัลแวร์)



รูปที่ 17 เลือกไฟล์ติดตั้งแบบ MSI 64-bit x86 จากหน้าดาวน์โหลด

ขั้นตอนที่ 2: เปิดไฟล์ติดตั้ง

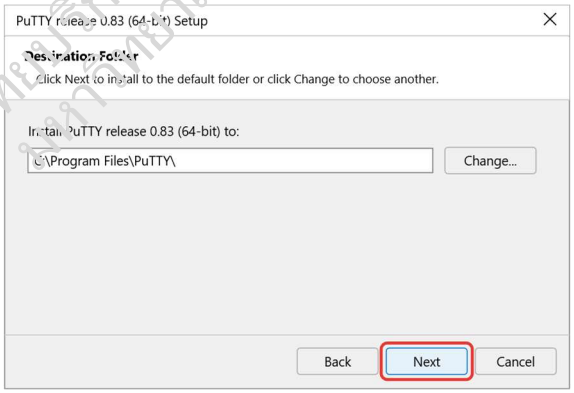
ไปที่โฟลเดอร์ Downloads แล้วดับเบิลคลิกไฟล์ putty-64bit-x.xx-installer.msi เมื่อหน้าต่าง Setup Wizard ปรากฏขึ้น ให้คลิก Next



รูปที่ 18 หน้าต้อนรับของ Setup Wizard

ขั้นตอนที่ 3: เลือกโฟลเดอร์ที่ติดตั้ง

โปรแกรมจะติดตั้งไว้ที่ C:\Program Files\PuTTY\ เป็นค่าเริ่มต้น ซึ่งแนะนำให้ใช้ค่านี้ หากต้องการเปลี่ยนตำแหน่งให้คลิก Change... จากนั้นคลิก Next

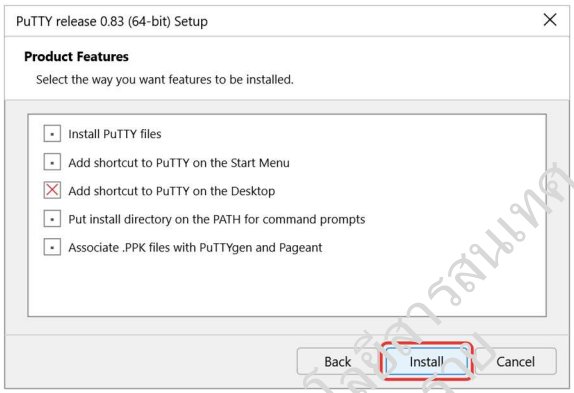


รูปที่ 19 หน้าเลือกโฟลเดอร์ที่ติดตั้ง

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏเชียงราย

ขั้นตอนที่ 4: เลือกส่วนประกอบที่ต้องการติดตั้ง

หน้า Product Features จะแสดงรายการส่วนประกอบของโปรแกรม แนะนำให้ใช้ค่าเริ่มต้น หากต้องการสร้างทางลัด (Shortcut) บนหน้าจอ Desktop ให้คลิกที่รายการ Add shortcut to PuTTY on the Desktop แล้วเลือกให้ติดตั้ง จากนั้นคลิก Install

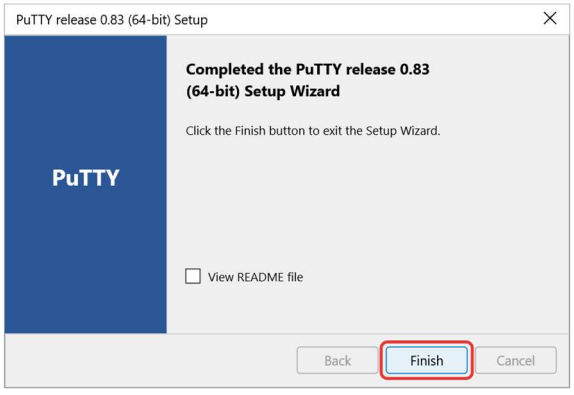


รูปที่ 20 หน้าเลือกส่วนประกอบ (Product Features)

(หาก Windows แสดงหน้าต่าง User Account Control ถามว่าอนุญาตให้แอปนี้ทำการเปลี่ยนแปลงหรือไม่ ให้คลิก Yes)

ขั้นตอนที่ 5: ติดตั้งเสร็จสิ้น

รอจนการติดตั้งเสร็จ เมื่อปรากฏหน้า Completed ให้เอาเครื่องหมายถูกที่ View README file ออกหากไม่ต้องการอ่านไฟล์คำอธิบาย แล้วคลิก Finish



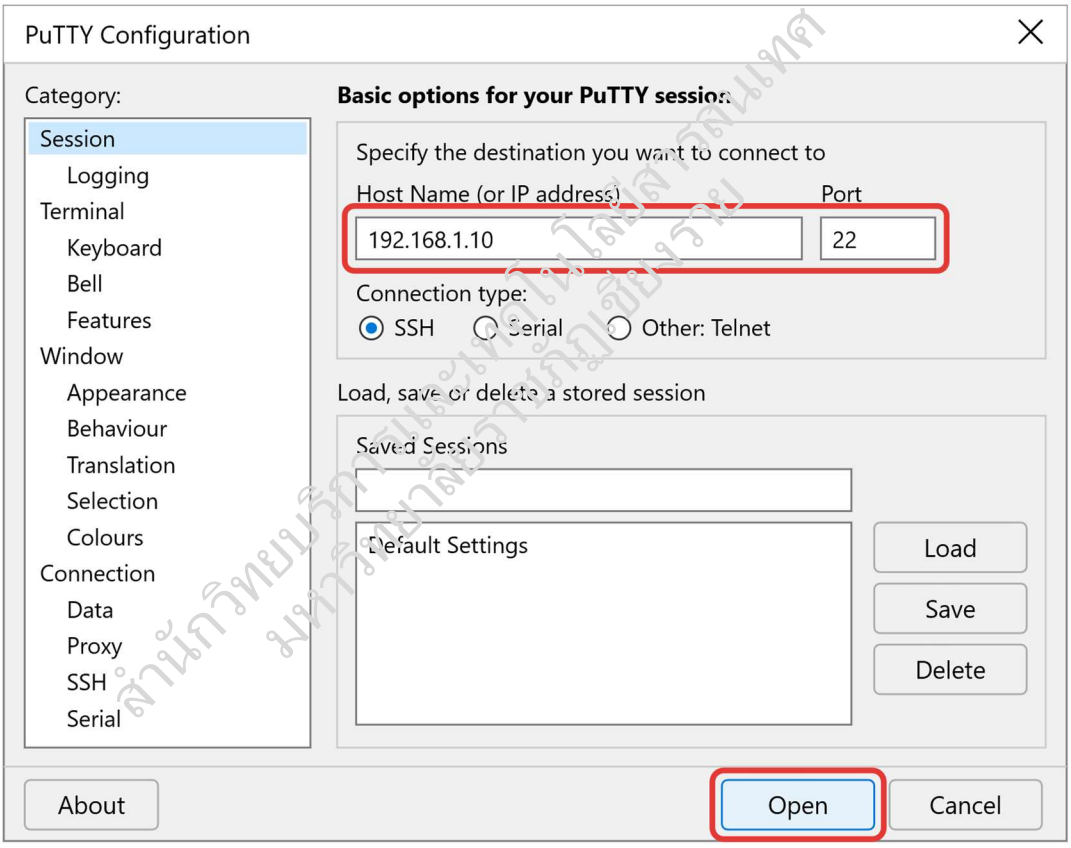
รูปที่ 21 หน้าจอเมื่อติดตั้งเสร็จสิ้น

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏเชียงราย

ขั้นตอนที่ 6: ทดสอบการเชื่อมต่อ

คลิกปุ่ม Start แล้วพิมพ์ PuTTY เพื่อเปิดโปรแกรม ในหน้า PuTTY Configuration ให้ทำดังนี้

1. ใส่ IP Address หรือชื่อเครื่องของเซิร์ฟเวอร์ในช่อง Host Name (or IP address)
2. ตรวจสอบว่าช่อง Port เป็น 22 และ Connection type เป็น SSH
3. คลิก Open
4. หากเชื่อมต่อครั้งแรก จะมีหน้าต่าง PuTTY Security Alert แจ้งเรื่อง host key ให้ตรวจสอบกับผู้ดูแลเซิร์ฟเวอร์แล้วคลิก Accept จากนั้นใส่ชื่อผู้ใช้และรหัสผ่านเพื่อเข้าสู่ระบบ



รูปที่ 22 หน้าต่าง PuTTY Configuration สำหรับเชื่อมต่อ SSH