



สถาบันดนตรีกัลยาณีวัฒนา
PRINCESS GALYANI VADHANA INSTITUTE OF MUSIC

คู่มือการปฏิบัติงาน
การออกแบบและการจัดการระบบเครือข่าย
คอมพิวเตอร์ของสถาบันดนตรีกัลยาณีวัฒนา

จัดทำโดย

นายพงศธร ศรีวิเศษ

งานเทคโนโลยีและสารสนเทศ

สถาบันดนตรีกัลยาณีวัฒนา

คำนำ

งานเทคโนโลยีและสารสนเทศ สำนักงานสถาบัน สถาบันดนตรีกัลยาณีวัฒนา ได้ดำเนินการจัดทำคู่มือปฏิบัติงานการออกแบบและการจัดการระบบเครือข่ายคอมพิวเตอร์ ของสถาบันดนตรีกัลยาณีวัฒนาเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงานในสถาบัน มีความเข้าใจในระบบเครือข่ายคอมพิวเตอร์ สามารถนำไปใช้ประกอบการปฏิบัติงานให้เกิดประสิทธิภาพ และเป็นไปในแนวทางเดียวกัน อีกทั้งสามารถช่วยเหลือหน่วยงานที่ขอรับบริการในการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ของสถาบันดนตรีกัลยาณีวัฒนา ได้อย่างถูกต้องอีกด้วย

ทางผู้จัดทำหวังเป็นอย่างยิ่งว่า คู่มือฉบับนี้จะเป็นประโยชน์แก่ผู้ปฏิบัติงานในสำนักงานเทคโนโลยีและสารสนเทศในการกำกับดูแลรักษาระบบเครือข่ายของสถาบันดนตรีกัลยาณีวัฒนา และผู้ที่เกี่ยวข้องนำไปช่วยในการปฏิบัติงานได้อย่างถูกต้อง และมีประสิทธิภาพ หากคู่มือฉบับนี้มีข้อผิดพลาดประการใด ทางผู้จัดทำขออภัยมา ณ ที่นี้ด้วย

พงศธร ศรีวิเศษ
กรกฎาคม 2568

สารบัญ

	หน้า
คำนำ.....	ก
สารบัญ.....	ข
สารบัญรูปภาพ.....	ค
สารบัญตาราง.....	ช
บทที่ 1 บทนำ.....	1
ความเป็นมา/ความจำเป็น/ความสำคัญ.....	1
วัตถุประสงค์.....	1
ขอบเขต.....	2
ประโยชน์ที่คาดว่าจะได้รับ.....	2
นิยามศัพท์เฉพาะ/คำจำกัดความ.....	2
บทที่ 2 โครงสร้างและหน้าที่ความรับผิดชอบ.....	3
โครงสร้างการบริหารจัดการ.....	3
บทบาทหน้าที่ความรับผิดชอบของตำแหน่ง.....	7
ลักษณะงานที่ปฏิบัติ.....	8
บทที่ 3 หลักเกณฑ์วิธีการปฏิบัติงานและเงื่อนไข.....	10
กฎหมาย ข้อบังคับ ระเบียบ ประกาศ หลักเกณฑ์ที่เกี่ยวข้องกับการปฏิบัติงาน.....	10
เงื่อนไข/ข้อสังเกต/ข้อควรระวัง/สิ่งที่ควรคำนึงในการปฏิบัติงาน.....	16
บทที่ 4 วิธีการปฏิบัติงาน.....	18
กิจกรรมและแผนการปฏิบัติงาน.....	18
ขั้นตอนในการปฏิบัติงาน.....	23
วิธีปฏิบัติงาน.....	25
วิธีการติดตามประเมินผลการปฏิบัติงาน	61
จรรยาบรรณ/คุณธรรม/จริยธรรมในการปฏิบัติงาน	62

สารบัญ (ต่อ)

	หน้า
บทที่ 5 ปัญหาอุปสรรคและแนวทางในการแก้ปัญหาและพัฒนางาน	63
ปัญหาอุปสรรคในการปฏิบัติงาน	63
แนวทางในการแก้ไขและพัฒนา	64
ข้อเสนอแนะ	65
บรรณานุกรม	66
ประวัติผู้เขียน	67

สารบัญรูปภาพ

	หน้า
ภาพที่ 2.1 โครงสร้างการแบ่งส่วนงานสถาบันดนตรีกัลยาณิวัฒนา	5
ภาพที่ 2.2 โครงสร้างการบริหาร (Administration Chart) สำนักงานสถาบัน	6
ภาพที่ 2.3 โครงสร้างการปฏิบัติงาน (Activity chart) งานเทคโนโลยีและสารสนเทศ	6
ภาพที่ 2.4 ขั้นตอนการปฏิบัติงาน	9
ภาพที่ 3.1 รูปการออกแบบเครือข่ายลักษณะ 3-Tier Design (สถาปัตยกรรมแบบ 3 ชั้น)	11
ภาพที่ 3.2 ตัวอย่างรูปแบบของ IP Address	13
ภาพที่ 3.3 รูปแบบโครงสร้างพื้นฐาน IP Address	13
ภาพที่ 3.4 รูปการออกแบบ VLAN ภายใน Switch	16
ภาพที่ 4.1 แผนผังระบบเครือข่ายคอมพิวเตอร์ ของสถาบันดนตรีกัลยาณิวัฒนา	18
ภาพที่ 4.2 แผนผังขั้นตอนการปฏิบัติงาน	24
ภาพที่ 4.3 ตัวอย่างบันทึกข้อความขออนุมัติปิดปรับปรุงระบบเครือข่ายคอมพิวเตอร์แผนการติดตั้ง ..	25
ภาพที่ 4.4 ประกาศปิดปรับปรุงระบบเครือข่ายคอมพิวเตอร์สถาบันดนตรีกัลยาณิวัฒนา.....	26
ภาพที่ 4.5 การแจ้งประกาศปิดปรับปรุงระบบเครือข่ายคอมพิวเตอร์ บน Application Line	26
ภาพที่ 4.6 ชุดเครื่องมือเบื้องต้นสำหรับ ติดตั้งสำหรับอุปกรณ์สวิตช์ (Switch)	27
ภาพที่ 4.7 ภาพแสดง Console Port แบบต่าง ๆ บนอุปกรณ์สวิตช์	28
ภาพที่ 4.8 ภาพแสดงการต่อสาย Console USB to DB 9 (Serial Port) เชื่อมต่อกับ สาย Serial Port (DB9) Female To Female	29
ภาพที่ 4.9 ภาพแสดงการกำหนดหมายเลขพอร์ตเมื่อต่อสาย Console USB to DB 9 (Serial Port) เชื่อมต่อกับ สาย Serial Port (DB9) To RJ45	29
ภาพที่ 4.10 ภาพแสดงการกำหนดหมายเลขพอร์ตเมื่อต่อสาย Console USB To RJ45	30
ภาพที่ 4.11 ภาพแสดงการกำหนดหมายเลขพอร์ตเมื่อต่อสาย Console USB	30
ภาพที่ 4.12 ภาพแสดงหน้าต่าง Application PuTTY ที่เชื่อมต่อแบบ Console USB	31
ภาพที่ 4.13 ภาพแสดงหน้าต่างคอนโซล PuTTY	31
ภาพที่ 4.14 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนชื่อผู้ใช้	31
ภาพที่ 4.15 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนรหัสผ่าน	32
ภาพที่ 4.16 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนชื่อผู้ใช้และป้อนรหัสผ่านสำเร็จ	32
ภาพที่ 4.17 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนรหัสผ่านไม่สำเร็จ	32

สารบัญรูปภาพ (ต่อ)

	หน้า
ภาพที่ 4.18 ภาพแสดงหน้าต่าง Application PuTTY ที่เชื่อมต่อแบบ Telnet	33
ภาพที่ 4.19 ภาพแสดงหน้าต่างคอนโซล PuTTY อินเทอร์เฟซบรรทัดคำสั่ง (CLI)	33
ภาพที่ 4.20 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนชื่อผู้ใช้	34
ภาพที่ 4.21 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนชื่อผู้ใช้และป้อนรหัสผ่าน	34
ภาพที่ 4.22 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนรหัสผ่านสำเร็จ	34
ภาพที่ 4.23 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนรหัสผ่านไม่สำเร็จ	34
ภาพที่ 4.24 ภาพแสดงหน้าต่าง Application PuTTY ที่เชื่อมต่อแบบ SSH	35
ภาพที่ 4.25 ภาพแสดงหน้าต่างคอนโซล PuTTY อินเทอร์เฟซบรรทัดคำสั่ง (CLI)	35
ภาพที่ 4.26 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนชื่อผู้ใช้	35
ภาพที่ 4.27 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนชื่อผู้ใช้และป้อนรหัสผ่าน	36
ภาพที่ 4.28 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนรหัสผ่านสำเร็จ	36
ภาพที่ 4.29 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนรหัสผ่านไม่สำเร็จ	36
ภาพที่ 4.30 แผนผังการเชื่อมต่อ Switch Access Layer เข้ากับ Switch Distribution Layer	37
ภาพที่ 4.31 อุปกรณ์สวิตช์ Cisco WS-C2960X-24PD-L	37
ภาพที่ 4.38 อุปกรณ์สวิตช์ Cisco SG300-28 28-Port 10/100/1000	40
ภาพที่ 4.33 การใช้คำสั่ง Ping ไปที่ ip gateway 192.168.99.1	46
ภาพที่ 4.34 การใช้คำสั่ง Ping จาก 192.168.99.111 ไปที่ IP Address 192.168.99.113.....	46
ภาพที่ 4.35 ใช้คำสั่ง show interfaces status เพื่อทำการตรวจสอบการตั้งค่าของ Cisco WS-C2960X-24PD-L	47
ภาพที่ 4.36 ใช้คำสั่ง show vlan เพื่อทำการตรวจสอบการตั้งค่าของ Cisco SG300-28	47
ภาพที่ 4.37 ป้อนที่อยู่เพื่อเข้าระบบ Monitoring	48
ภาพที่ 4.38 หน้าต่างระบบ Monitoring (ZABBIX) พร้อมเข้าสู่ระบบ	48
ภาพที่ 4.39 หน้าต่างระบบ Monitoring (ZABBIX) การป้อนชื่อผู้ใช้และรหัสผ่าน	48
ภาพที่ 4.40 หน้าต่างระบบ Monitoring (ZABBIX) หลังจากการเข้าสู่ระบบสำเร็จ	49
ภาพที่ 4.41 หน้าต่างการแจ้งเตือนหลังจากการเข้าสู่ระบบไม่สำเร็จ	49
ภาพที่ 4.42 การแสดงเมนูบนระบบ Monitoring (ZABBIX)	50
ภาพที่ 4.43 การแสดงเมนูบนระบบ Monitoring (ZABBIX) ในส่วน Data collection	50

สารบัญรูปภาพ (ต่อ)

	หน้า
ภาพที่ 4.44 การแสดงเมนูบนระบบ Monitoring (ZABBIX) เมนูย่อย Host ของเมนู Data collection	51
ภาพที่ 4.45 การแสดงเมนูบนระบบ Monitoring (ZABBIX) ปุ่ม Create Host	51
ภาพที่ 4.46 หน้าระบบที่ชื่อว่า New Host	52
ภาพที่ 4.47 หน้าระบบการป้อนข้อมูลอุปกรณ์สวิชท์	52
ภาพที่ 4.48 หน้าระบบการป้อนชื่ออุปกรณ์สวิชท์	53
ภาพที่ 4.49 หน้าระบบการเพิ่ม Templates	53
ภาพที่ 4.50 หน้าระบบรายการ Templates	54
ภาพที่ 4.51 หน้าระบบรายการเลือก Templates	54
ภาพที่ 4.52 หน้ารายการ Templates ของ Network devices	55
ภาพที่ 4.53 หน้าเพิ่มข้อมูล Templates	55
ภาพที่ 4.53 หน้าการเพิ่ม Host groups	56
ภาพที่ 4.55 หน้ารายการ Host groups	56
ภาพที่ 4.56 เพิ่มข้อมูล Host groups	57
ภาพที่ 4.57 การตั้งค่า Interfaces	57
ภาพที่ 4.58 การตั้งค่าประเภทการส่งข้อมูล	58
ภาพที่ 4.59 การแสดงช่องสำหรับป้อนข้อมูลการส่งข้อมูล	58
ภาพที่ 4.60 การตั้งค่าป้อนข้อมูลการส่งข้อมูล	59
ภาพที่ 4.60 การแสดงข้อมูลในหน้าแสดงข้อมูลของอุปกรณ์ทั้งหมดที่มีในระบบ	60

สารบัญตาราง

	หน้า
ตารางที่ 3.1 ตารางการแบ่ง Subnet แบบตรง Octet (N=Network, H=Host).....	14
ตารางที่ 3.2 ตารางการแบ่ง Subnet แบบที่ไม่ตรงกับ Octet.....	15
ตารางที่ 4.1 การใช้หมายเลขไอพีแอดเดรส รุ่น4 (IPV4) แบบ Private Network สำหรับกำหนดให้แก่อุปกรณ์คอมพิวเตอร์สำหรับผู้ใช้งานใน Building Zone.....	14
ตารางที่ 4.2 การใช้หมายเลขไอพีแอดเดรส รุ่น4 (IPV4) แบบ Private Network สำหรับกำหนดให้แก่อุปกรณ์ Access Point (แอคเซสพอยต์) ใน WIFI Zone.....	21
ตารางที่ 4.3 การใช้หมายเลขไอพีแอดเดรส รุ่น4 (IPV4) แบบ Private Network สำหรับกำหนดให้แก่อุปกรณ์ Network Switch ประจำ Building Zone.....	21
ตารางที่ 4.4 การใช้หมายเลขไอพีแอดเดรส รุ่น4 (IPV4) แบบ Private Network สำหรับกำหนดให้แก่อุปกรณ์ Network ที่ทำการติดตั้งภายในห้อง Data Center.....	21
ตารางที่ 4.5 การใช้หมายเลขไอพีแอดเดรส รุ่น4 (IPV4) แบบ Private Network สำหรับกำหนดให้แก่อุปกรณ์คอมพิวเตอร์ Server ประจำ Server Zone.....	22
ตารางที่ 4.6 การใช้หมายเลขไอพีแอดเดรส รุ่น4 (IPV4) แบบ Private Network สำหรับกำหนดให้แก่ระบบ VPN (Virtual Private Network).....	22
ตารางที่ 4.7 การใช้หมายเลขไอพีแอดเดรส รุ่น4 (IPV4) แบบ Private Network สำหรับกำหนดให้แก่อุปกรณ์อื่น ๆ.....	22
ตารางที่ 4.8 ตารางแผนการปฏิบัติงาน.....	23

บทที่ 1

บทนำ

1.1 ความเป็นมา/ความจำเป็น/ความสำคัญ

ปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสาร มีบทบาทสำคัญอย่างยิ่งในภาคการศึกษา โดยเฉพาะอย่างยิ่งในสถาบันการศึกษาที่ต้องการเพิ่มประสิทธิภาพในการเรียนการสอน การบริหารจัดการ และการให้บริการต่าง ๆ แก่ นักศึกษา อาจารย์ และพนักงานสถาบัน สถาบันดนตรีกัลยาณีวัฒนาในฐานะสถาบันเฉพาะทางด้านดนตรี จำเป็นต้องมีระบบเครือข่ายคอมพิวเตอร์ที่มั่นคงปลอดภัย และมีประสิทธิภาพสูงเพื่อสนับสนุนกิจกรรมด้านวิชาการ การฝึกปฏิบัติ และการบริหารภายในให้สอดคล้องกับมาตรฐานสากล

ผู้จัดทำได้จัดทำคู่มือปฏิบัติงาน เรื่อง ออกแบบและการจัดการระบบเครือข่ายคอมพิวเตอร์ของสถาบันดนตรีกัลยาณีวัฒนา คู่มือปฏิบัติงานฉบับนี้เกิดจากความต้องการในการออกแบบวางระบบ และบริหารจัดการโครงสร้างพื้นฐานของระบบเครือข่ายคอมพิวเตอร์ภายในสถาบันให้มีความเป็นระบบมีขั้นตอนชัดเจน และสามารถตรวจสอบได้ นอกจากนี้ยังเป็นการเตรียมความพร้อมสู่การรองรับเทคโนโลยีใหม่ ๆ เช่น ระบบห้องเรียนอัจฉริยะ (Smart Classroom), การเรียนออนไลน์ และระบบบริหารจัดการข้อมูลส่วนกลางของสถาบัน ซึ่งต้องอาศัยโครงข่ายที่มีประสิทธิภาพเป็นพื้นฐานสำคัญ

คู่มือฉบับนี้จึงมีความสำคัญต่อผู้ปฏิบัติงานด้านเทคโนโลยีคอมพิวเตอร์ เพื่อเป็นแนวทางในการดำเนินงานตั้งแต่ขั้นตอนการวางแผน ออกแบบระบบ ไปจนถึงการดูแลบำรุงรักษา ตลอดจนสามารถใช้เป็นเครื่องมือในการประเมินความพร้อมของระบบเครือข่ายที่มีอยู่ และวางแผนการปรับปรุงในอนาคตได้อย่างเป็นระบบ

1.2 วัตถุประสงค์

1. เพื่อกำหนดแนวทางการออกแบบและจัดการระบบเครือข่ายคอมพิวเตอร์ของสถาบันดนตรีกัลยาณีวัฒนาให้เป็นมาตรฐาน
2. เพื่อให้บุคลากรผู้เกี่ยวข้องสามารถปฏิบัติงานด้านระบบเครือข่ายได้อย่างมีประสิทธิภาพ และลดข้อผิดพลาดในการดำเนินงาน

1.3 ขอบเขต

คู่มือปฏิบัติงาน เรื่อง ออกแบบและจัดการระบบเครือข่ายคอมพิวเตอร์ของสถาบันดนตรี วิทยาลัยพัฒนา ครอบคลุมกระบวนการออกแบบและบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ภายใน สถาบันดนตรีวิทยาลัยพัฒนา โดยเน้นถึงการกำหนดโครงสร้างเครือข่ายแบบมีสายและไร้สาย การติดตั้งอุปกรณ์เครือข่าย เช่น Switch, Firewall และ Wireless Access Point การจัดการ IP Address และการบำรุงรักษาเครือข่าย รวมถึงระบบสำรองข้อมูลและการกู้คืนข้อมูลในกรณีฉุกเฉิน ทั้งนี้ ไม่ครอบคลุมถึงการพัฒนาโปรแกรมประยุกต์หรือซอฟต์แวร์ที่ใช้ภายในสถาบัน

1.4 ประโยชน์ที่คาดว่าจะได้รับ

- 1) ผู้ปฏิบัติงานเทคโนโลยีคอมพิวเตอร์กำหนดแนวทางการออกแบบและจัดการระบบเครือข่ายคอมพิวเตอร์ของสถาบันดนตรีวิทยาลัยพัฒนาให้เป็นมาตรฐาน
- 2) ผู้ปฏิบัติฝ่ายเทคโนโลยีคอมพิวเตอร์สามารถปฏิบัติงานด้านระบบเครือข่ายได้อย่างมีประสิทธิภาพ และลดข้อผิดพลาดในการดำเนินงาน

1.5 นิยามศัพท์เฉพาะ/คำจำกัดความ

สถาบัน หมายถึง สถาบันดนตรีวิทยาลัยพัฒนา

พนักงานสถาบัน หมายถึง พนักงานสถาบันดนตรีวิทยาลัยพัฒนา

สำนักงานสถาบัน หมายถึง สำนักงานสถาบันดนตรีวิทยาลัยพัฒนา

สำนักวิชา หมายถึง สำนักวิชาดุริยางคศาสตร์

ผู้ปฏิบัติงาน หมายถึง พนักงานสถาบัน และลูกจ้างของสถาบัน

ฝ่ายเทคโนโลยีคอมพิวเตอร์ หมายถึง ฝ่ายเทคโนโลยีคอมพิวเตอร์ สำนักงานสถาบัน เป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบ คอมพิวเตอร์และเครือข่ายภายในสถาบัน

ระบบเครือข่าย (Network) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูล และ สารสนเทศ ระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของสถาบัน ได้แก่

ระบบ LAN หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อ ระบบคอมพิวเตอร์ต่าง ๆ ภายในสถาบันเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยน ข้อมูลและ สารสนเทศภายในสถาบัน

ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อ ระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของสถาบันเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

วีแลน (VLAN) หมายถึง เทคโนโลยีเครือข่ายที่ช่วยในการแบ่งเครือข่ายทางกายภาพ (Physical Network) ออกเป็นเครือข่ายตรรกะหรือเครือข่ายเสมือนย่อยๆ หลายเครือข่าย ภายในเครือข่ายกายภาพเดียวกัน โดยไม่จำเป็นต้องแยกอุปกรณ์ทางกายภาพออกจากกัน

เลขที่อยู่ไอพี (IP Address) หมายถึง ชุดตัวเลขที่ใช้ในการระบุเครื่องคอมพิวเตอร์หรืออุปกรณ์ในระบบเครือข่าย

Firewall หมายถึง ระบบที่ช่วยป้องกันและควบคุมการเข้าถึงเครือข่ายจากภายนอก เพื่อความปลอดภัยของข้อมูลภายใน

Bandwidth หมายถึง ความสามารถของระบบเครือข่ายในการส่งข้อมูลในช่วงเวลาหนึ่ง มีหน่วยวัดเป็น Mbps หรือ Gbps

Access Point (AP) หมายถึง อุปกรณ์ที่เชื่อมต่อกับระบบ LAN เพื่อกระจายสัญญาณอินเทอร์เน็ตแบบไร้สายให้กับผู้ใช้งาน

บทที่ 2

โครงสร้างและหน้าที่ความรับผิดชอบ

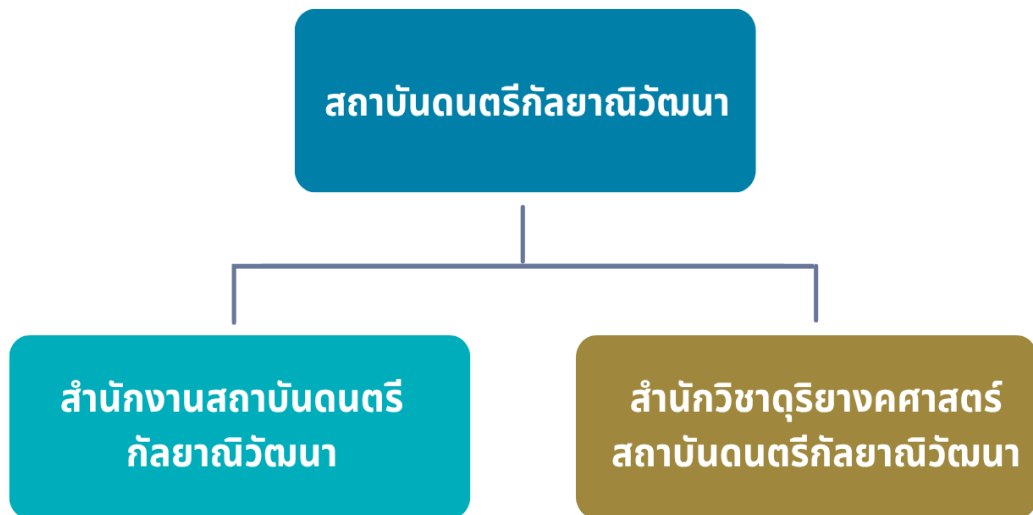
2.1 โครงสร้างการบริหารจัดการ

โครงการจัดตั้งสถาบันดนตรีกัลยาณิวัฒนา ที่ประชุมคณะรัฐมนตรีชุดพลเอกสุรยุทธ์ จุลานนท์ ได้ให้ความเห็นชอบโครงการจัดตั้งสถาบันดนตรีกัลยาณิวัฒนาเป็นโครงการเฉลิมพระเกียรติสมเด็จพระเจ้าพี่นางเธอ เจ้าฟ้ากัลยาณิวัฒนา กรมหลวงนราธิวาสราชนครินทร์ ในวโรกาสทรงเจริญพระชนมายุ 7 รอบ 6 พฤษภาคม พ.ศ. 2550 เมื่อ 11 กรกฎาคม พ.ศ. 2550 ในการประชุมครั้งที่ 4/2550 สภามหาวิทยาลัยศิลปากร ได้เห็นชอบโครงการจัดตั้งสถาบันดนตรีกัลยาณิวัฒนาเป็นหน่วยงานในกำกับของมหาวิทยาลัยศิลปากร ตามที่สำนักงบประมาณได้เสนอแนะ เพื่อให้สามารถขอ งบประมาณแผ่นดินมาดำเนินการในการจัดตั้งสถาบันดนตรีกัลยาณิวัฒนาได้ และกระทรวงวัฒนธรรม ได้มีหนังสือขอความอนุเคราะห์กระทรวงอุตสาหกรรม ขอใช้พื้นที่ 14 ไร่ บริเวณโรงงานสุราบางยี่ขัน เดิมเชิงสะพานพระราม 8 ฝั่งธนบุรี เพื่อใช้เป็นพื้นที่จัดตั้งสถาบันดนตรีกัลยาณิวัฒนา วันที่ 25 ธันวาคม พ.ศ. 2550 ที่ประชุมคณะรัฐมนตรีเห็นชอบให้จัดตั้งสถาบันดนตรีกัลยาณิวัฒนา โดยจัดตั้ง เป็นนิติบุคคลมีฐานะเป็นหน่วยงานในกำกับของรัฐ ดำเนินงานโดยเป็นสถานศึกษาทางวิชาการและ วิชาชีพชั้นสูง มีวัตถุประสงค์เพื่อให้การศึกษา ส่งเสริม พัฒนาวิชาการ และวิชาชีพชั้นสูงในทางดนตรี และศาสตร์อื่นที่เกี่ยวข้อง ทำการสอน ทำการวิจัย ให้บริการทางวิชาการแก่สังคมและทำนุบำรุง ศิลปวัฒนธรรม เพื่อประโยชน์ต่อการพัฒนาชุมชน สังคม และประเทศชาติ ซึ่งในการจัดทำคู่มือฉบับนี้ ผู้เขียนได้เรียบเรียงโครงสร้างแบ่งเป็น 3 รูปแบบ ดังนี้

- 1) โครงสร้างองค์กร (Organization chart)
- 2) โครงสร้างการบริหาร (Administration Chart)
- 3) โครงสร้างการปฏิบัติงาน (Activity chart)

2.1.1 โครงสร้างองค์กร (Organization chart) ของสถาบันดนตรีกัลยาณิวัฒนา

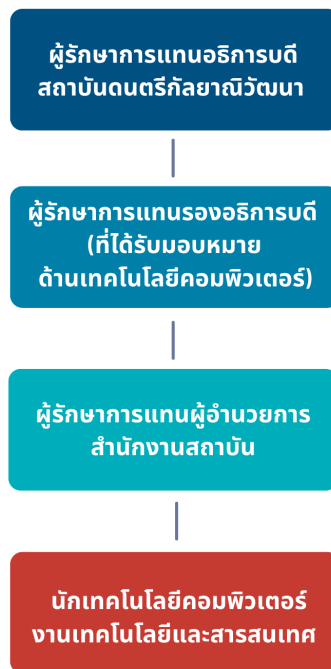
โครงสร้างการบริหารจัดการองค์กรของสถาบันดนตรีกัลยาณิวัฒนา กำหนดไว้ในตาม พระราชบัญญัติสถาบันดนตรีกัลยาณิวัฒนา พ.ศ. 2555 ตามมาตรา 4 มีฐานะเป็นหน่วยงานในกำกับ ของรัฐ และมาตรา 7 สถาบันอาจแบ่งส่วนงาน ดังนี้ (1) สำนักงานสถาบัน (2) สำนักวิชา (3) ส่วนงาน อื่น ดังแสดงในภาพที่ 2.1



ภาพที่ 2.1 โครงสร้างการแบ่งส่วนงานสถาบันดนตรีกลายาณวัฒนา

2.1.2 โครงสร้างการบริหาร (Administration Chart) สำนักงานสถาบัน

สำนักงานสถาบันได้แบ่งกลุ่มงานตามประกาศสถาบันสถาบันดนตรีกลายาณวัฒนา เรื่องการแบ่งกลุ่มงานภายในของสำนักงานสถาบันดนตรีกลายาณวัฒนา พ.ศ. 2565 โดยแบ่งเป็นกลุ่มงาน จำนวน 4 กลุ่มงาน ประกอบด้วย กลุ่มงานบริหารกลาง กลุ่มงานยุทธศาสตร์แผนและงบประมาณ และกลุ่มงานบริการวิชาการ และมีประกาศสถาบันสถาบันดนตรีกลายาณวัฒนา เรื่อง การแบ่งกลุ่มงานภายในของสำนักงานสถาบันดนตรีกลายาณวัฒนา (ฉบับที่ 2) พ.ศ. 2566 สำหรับกลุ่มงานบริหารกลาง ได้แบ่งภารกิจของหน่วยงานเป็น 5 งาน ประกอบด้วย งานบริหารบุคคลและกฎหมาย สารบรรณ งานประชุมและพิธีการ งานเทคโนโลยีและสารสนเทศ, ประชาสัมพันธ์และงานวิเทศสัมพันธ์ งานอาคารสถานที่และยานพาหนะ เมื่อวันที่ 18 มิถุนายน พ.ศ. 2568 ดังแสดงในภาพที่ 2.2



ภาพที่ 2.2 โครงสร้างการบริหาร (Administration Chart) สำนักงานสถาบัน

2.1.3 โครงสร้างการปฏิบัติงาน (Activity chart) ของงานเทคโนโลยีและสารสนเทศ



ภาพที่ 2.3 โครงสร้างการปฏิบัติงาน (Activity chart) งานเทคโนโลยีและสารสนเทศ

2.2 บทบาทหน้าที่ความรับผิดชอบของตำแหน่ง

หน้าที่ความรับผิดชอบของตำแหน่งตามมาตรฐานกำหนดตำแหน่ง

ตามประกาศสถาบันดนตรีกัลยาณีวัฒนา เรื่อง กำหนดตำแหน่งและมาตรฐานกำหนดตำแหน่งของพนักงานสถาบันดนตรีกัลยาณีวัฒนา พ.ศ. 2567 เมื่อวันที่ 22 กุมภาพันธ์ 2567 โดยระบุบทบาทหน้าที่ความรับผิดชอบของ ตำแหน่งพนักงานสถาบันประเภทปฏิบัติการวิชาชีพ ระดับตำแหน่ง ปฏิบัติการวิชาชีพ 3 (ค่างานระดับ 3) มีหน้าที่ ความรับผิดชอบหลัก ดังนี้

ปฏิบัติงานในฐานะผู้ปฏิบัติงานระดับต้นที่ต้องใช้ความรู้ความสามารถทางวิชาการในการทำงาน ปฏิบัติงานเกี่ยวกับเทคโนโลยีสารสนเทศหรือวิทยาการคอมพิวเตอร์ ภายใต้การกำกับ แนะนำ ตรวจสอบ และ ปฏิบัติงานอื่นตามที่ได้รับมอบหมาย โดยมีลักษณะงานที่ปฏิบัติในด้านต่างๆ ดังนี้

2.2.1 ด้านการปฏิบัติการ

1) ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ที่เกี่ยวข้อง ระบบเครือข่ายคอมพิวเตอร์ ทดสอบคุณสมบัติด้านเทคนิคของระบบ ติดตั้งชุดคำสั่งระบบปฏิบัติการ ชุดคำสั่งสำเร็จรูป เพื่ออำนวยความสะดวกให้งานเทคโนโลยีและสารสนเทศในความรับผิดชอบดำเนินไปได้อย่างราบรื่น และสอดคล้องกับความต้องการของหน่วยงาน

2) ประมวลผล และปรับปรุงแก้ไขแฟ้มข้อมูล เขียนชุดคำสั่ง และคู่มือคำอธิบายชุดคำสั่งตามข้อกำหนดของระบบงานที่ได้วางแผนไว้แล้ว ทดสอบความถูกต้องของคำสั่ง แก้ไขข้อผิดพลาดของคำสั่งเพื่อให้ระบบปฏิบัติการทำงานได้อย่างถูกต้องแม่นยำและมีประสิทธิภาพมากที่สุด

3) ให้บริการวิชาการด้านต่างๆ เช่น ช่วยสอน ถ่ายทอดเทคโนโลยีในสาขาวิทยาการคอมพิวเตอร์ ให้คำปรึกษา แนะนำในการปฏิบัติงานแก่เจ้าหน้าที่ระดับรองลงมาและแก่นักศึกษาที่มาฝึกปฏิบัติงาน ตอบปัญหาและชี้แจงเรื่องต่างๆ เกี่ยวกับงานในหน้าที่ เพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง มีประสิทธิภาพ และปฏิบัติหน้าที่อื่นที่เกี่ยวข้อง

4) ศึกษา วิเคราะห์ รวบรวมข้อมูล สถิติ สรุปรายงาน เพื่อสนับสนุนการบริหารสำนักงาน ใน ด้านต่างๆ หรือจัดทำโครงการต่าง ๆ ให้สอดคล้องกับนโยบายของส่วนงานและสถาบัน

5) ประสานงานกับหน่วยงานและบุคคลต่างๆ ทั้งในประเทศและต่างประเทศเพื่ออำนวยความสะดวก และเกิดความร่วมมือร่วมกัน

6) ให้บริการด้านต่างๆ เช่น ให้คำปรึกษา แนะนำ ในการปฏิบัติงานแก่เจ้าหน้าที่ระดับรองลงมาและแก่นักศึกษาที่มาฝึกปฏิบัติงาน ตอบปัญหาและชี้แจงเรื่องต่างๆ เกี่ยวกับงานในหน้าที่ เพื่อให้สามารถ ปฏิบัติงานได้ถูกต้อง มีประสิทธิภาพ และปฏิบัติหน้าที่อื่นที่เกี่ยวข้อง

7) เข้าร่วมประชุมและดำเนินการในคณะกรรมการต่างๆ ที่ได้รับแต่งตั้ง

8) ให้ข้อมูลและบทวิเคราะห์สำหรับงานประกันคุณภาพ ในตัวชี้วัดที่เกี่ยวข้อง

9) ปฏิบัติงานอื่นๆ ตามที่ได้รับมอบหมายจากผู้บังคับบัญชา

2.2.2 ด้านการวางแผน

- 1) วางแผนการทำงานที่รับผิดชอบ ร่วมวางแผนการทำงานของหน่วยงานหรือโครงการ เพื่อให้การดำเนินงานบรรลุตามเป้าหมายและผลสัมฤทธิ์ที่กำหนด
- 2) ติดตามประเมินผลการดำเนินงาน จัดทำสรุป วิเคราะห์ และรายงานตัวชี้วัดตามแผน

2.2.3 ด้านการประสานงาน

- 1) ประสานการทำงานร่วมกันระหว่างทีมงานหรือหน่วยงานทั้งภายในและภายนอก เพื่อให้เกิดความร่วมมือและผลสัมฤทธิ์ตามที่กำหนดไว้
- 2) ชี้แจงและให้รายละเอียดเกี่ยวกับข้อมูล ข้อเท็จจริง แก่บุคคลหรือหน่วยงานที่เกี่ยวข้อง เพื่อสร้างความเข้าใจหรือความร่วมมือในการดำเนินงานตามที่ได้รับมอบหมาย

2.2.4 ด้านการบริการ

- 1) ให้คำปรึกษา แนะนำเบื้องต้น เผยแพร่ ถ่ายทอดความรู้ รวมทั้งตอบปัญหาและชี้แจงเรื่อง ต่างๆ เกี่ยวกับงานในหน้าที่ เพื่อให้ผู้รับบริการได้รับทราบข้อมูล ความรู้ต่างๆ ที่เป็นประโยชน์
- 2) จัดเก็บข้อมูลเบื้องต้นในงานที่เกี่ยวข้อง เพื่อให้บุคลากรทั้งภายในและภายนอกหน่วยงาน นักศึกษา ตลอดจนผู้รับบริการ ได้ทราบข้อมูลและความรู้ต่างๆ ที่เป็นประโยชน์ สอดคล้อง และสนับสนุนภารกิจ ของหน่วยงาน และใช้ประกอบการพิจารณากำหนดนโยบาย แผนงาน หลักเกณฑ์ มาตรการต่าง ๆ

2.3 ลักษณะงานที่ปฏิบัติ

บทบาทหน้าที่ความรับผิดชอบของนายพงศธร ศรีวิเศษ ตำแหน่งนักเทคโนโลยีคอมพิวเตอร์ ระดับ ปฏิบัติการวิชาชีพ 3 (ค่างานระดับ 3) ตามที่ได้รับมอบหมาย มีดังนี้

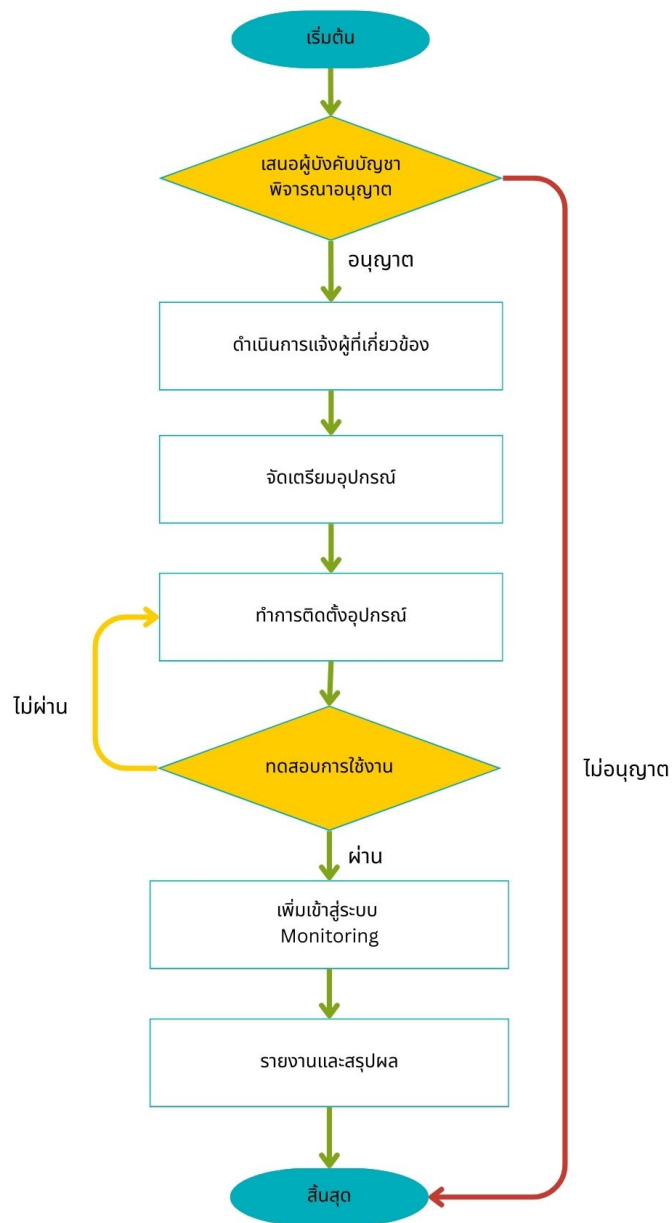
มีหน้าที่และความรับผิดชอบดังนี้

ปฏิบัติงานในฐานะผู้ปฏิบัติงานระดับ ปฏิบัติการวิชาชีพ 3 ทำหน้าที่รับผิดชอบ

- 1) ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ที่เกี่ยวข้อง ระบบเครือข่ายคอมพิวเตอร์
- 2) ดูแล บำรุงรักษา และติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย
- 3) วิเคราะห์กำหนดลักษณะและออกแบบระบบเครือข่าย (Network)
- 4) ดูแล บำรุงรักษา และติดตั้งระบบเครือข่าย (Network) ของสถาบัน
- 5) เขียนชุดคำสั่งที่ยุ่งยาก ซับซ้อน และคู่มือคำอธิบายชุดคำสั่ง
- 6) จัดการรหัสผู้ใช้งานระบบคอมพิวเตอร์ เช่น รหัสInternet , e-mail, Microsoft Office 365, Zoom, Software License เป็นต้น
- 7) ติดตามประเมินผลการดำเนินงาน จัดทำสรุป วิเคราะห์ และรายงานตัวชี้วัดตามแผน

- 8) ชี้แจงเรื่องต่างๆ ด้านเทคโนโลยีสารสนเทศในการปฏิบัติงานแก่พนักงานสถาบัน
- 9) นำเสนอความเห็นข้อเสนอแนะ และ ให้คำปรึกษาแก่ผู้บังคับบัญชา
- 10) ปฏิบัติหน้าที่อื่นที่เกี่ยวข้องในงานเทคโนโลยีและสารสนเทศ

จากภาระหน้าที่ที่ได้รับมอบหมายดังกล่าวข้างต้น ผู้เขียนได้เลือกภาระงานการออกแบบและ การจัดการระบบเครือข่ายคอมพิวเตอร์ ของสถาบันดนตรีกัลยาณีวัฒนา มาเขียนคู่มือการปฏิบัติงาน โดยมี ขั้นตอนการปฏิบัติงาน ดังนี้



ภาพที่ 2.4 ขั้นตอนการปฏิบัติงาน

บทที่ 3

หลักเกณฑ์วิธีการปฏิบัติงานและเงื่อนไข

3.1 หลักเกณฑ์ที่เกี่ยวข้องกับการปฏิบัติงาน

การออกแบบระบบเครือข่ายที่ดีควรยึดความต้องการใช้งานเป็นหลัก เน้นการใช้ประโยชน์จากเทคโนโลยีอย่างเต็มที่ ลดความซับซ้อนของระบบ เพื่อให้ง่ายต่อการบำรุงรักษา อัปเดต และขยายระบบในอนาคต โดยมีหลักการสำคัญคือการศึกษาและวิเคราะห์ความต้องการทั้งจากผู้ใช้งาน ผู้บริหาร และเทคโนโลยีอย่างรอบด้าน คู่มือการปฏิบัติงานเรื่องการออกแบบและการจัดการระบบเครือข่ายคอมพิวเตอร์ ของสถาบันดนตรีกัลยาณีวัฒนา มีหลักการที่เกี่ยวข้องดังนี้

- 3.1.1 แนวคิดและหลักการการออกแบบระบบเครือข่าย
- 3.1.2 หลักการทฤษฎีและมาตรฐานที่เกี่ยวข้องกับระบบเครือข่าย
- 3.1.3 หมายเลขไอพี (IP Address)
- 3.1.4 VLAN หรือ Virtual Local Area Network
- 3.1.5 การจัดการระบบเครือข่ายคอมพิวเตอร์

3.1.1 แนวคิดและหลักการการออกแบบระบบเครือข่าย

การวิเคราะห์ความต้องการ (Requirements Analysis)

- การศึกษาระบบเครือข่ายเดิม คือ ทำความเข้าใจสภาพแวดล้อมและข้อจำกัดของระบบเดิม
- การวิเคราะห์ความต้องการจากผู้ใช้งาน คือ เก็บข้อมูลเกี่ยวกับการใช้งานและความต้องการส่วนบุคคลของแต่ละบุคคลหรือกลุ่มผู้ใช้
- การวิเคราะห์ความต้องการขององค์กร คือ ทำความเข้าใจเป้าหมายและทิศทางขององค์กรที่เกี่ยวข้องกับระบบเครือข่าย.
- การวิเคราะห์ความต้องการด้านเทคโนโลยี คือ พิจารณาเทคโนโลยีที่ทันสมัยและเหมาะสมกับความต้องการที่เป็นไปได้

การศึกษาความเป็นไปได้ (Feasibility Study)

การประเมินความเป็นไปได้ในการออกแบบระบบเครือข่ายตามความต้องการที่ได้รวบรวมมา เพื่อให้เหมาะสมกับความต้องการที่เป็นไปได้ในการออกแบบระบบเครือข่าย

การเลือกประเภทของเครือข่าย (Network Type Selection)

การเลือกประเภทเครือข่ายที่เหมาะสมกับขนาดและลักษณะการใช้งานเป็นสิ่งสำคัญ เพื่อให้ได้ประสิทธิภาพสูงสุดและประหยัดค่าใช้จ่าย

การออกแบบโครงสร้างพื้นฐาน (Infrastructure Design)

- การออกแบบ Topology เป็นกำหนดโครงสร้างการเชื่อมต่ออุปกรณ์ให้เหมาะสม เช่น การเชื่อมต่อระดับ Core Layer เป็นส่วนที่มีความเร็วสูงที่สุดในระบบเครือข่ายหลักอุปกรณ์เครือข่าย ที่อยู่ในส่วนนี้ จะส่งข้อมูลได้รวดเร็วมีความน่าเชื่อถือสูง มีการติดตั้งแบบทดแทนกันได้

- การจัดการ Bandwidth คือ พิจารณาความต้องการแบนด์วิดท์ สำหรับแอปพลิเคชันต่าง ๆ

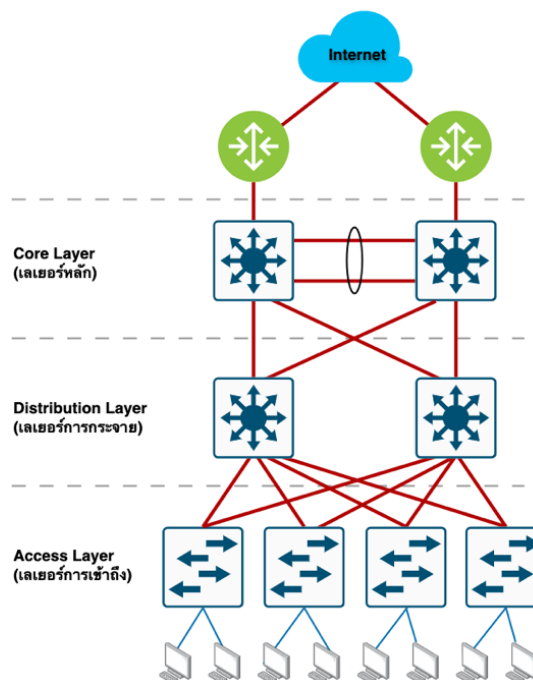
- การใช้ประโยชน์จากเทคโนโลยี คือ เลือกใช้เทคโนโลยีและพีเจอร์ที่เหมาะสม เพื่อเพิ่มประสิทธิภาพและลดความซับซ้อน

- ความยืดหยุ่นและการขยายตัว คือ ออกแบบให้สามารถอัปเดต แก้ไข หรือเพิ่มอุปกรณ์ใหม่ ๆ ได้ง่ายในอนาคต

- ความปลอดภัย คือ คำนึงถึงมาตรการรักษาความปลอดภัยของข้อมูล

3.1.2 หลักการทฤษฎีและมาตรฐานที่เกี่ยวข้องกับระบบเครือข่าย

การออกแบบเครือข่ายลักษณะ 3-Tier Design (สถาปัตยกรรมแบบ 3 ชั้น) เป็นหนึ่งในสถาปัตยกรรมที่ได้รับความนิยมในการออกแบบ Data Center โดยแบ่งออกเป็นสามชั้นหลัก โครงสร้างของเครือข่ายที่แบ่งออกเป็นสามเลเยอร์หลัก ได้แก่ Access Layer, Distribution Layer และ Core Layer ซึ่งเป็นโมเดลการออกแบบเครือข่ายที่ช่วยให้การจัดการเครือข่ายเป็นไปอย่างมีประสิทธิภาพและสามารถขยายได้อย่างง่ายดาย



ภาพที่ 3.1 รูปการออกแบบเครือข่ายลักษณะ 3-Tier Design (สถาปัตยกรรมแบบ 3 ชั้น)

1. Access Layer (เลเยอร์การเข้าถึง)

Access Layer เป็นชั้นที่ใกล้ชิดกับผู้ใช้งานมากที่สุด โดยทำหน้าที่เชื่อมต่ออุปกรณ์ผู้ใช้ เช่น คอมพิวเตอร์, โทรศัพท์ IP, และอุปกรณ์ IoT เข้ากับเครือข่ายอุปกรณ์ใน Access Layer มักจะเป็น สวิตช์ (Switch) ที่มีพอร์ตจำนวนมากเพื่อรองรับการเชื่อมต่อของอุปกรณ์หลายชนิด

Access Layer ยังเป็นจุดที่ใช้ในการควบคุมการเข้าถึงของผู้ใช้ โดยใช้เทคโนโลยีเช่น VLANs และ Port Security เพื่อจัดการความปลอดภัยและการจัดลำดับทราฟฟิก

2. Distribution Layer (เลเยอร์การกระจาย)

Distribution Layer ทำหน้าที่รวมทราฟฟิกจาก Access Layer หลาย ๆ ตัวเข้าด้วยกัน และเตรียมทราฟฟิกเหล่านั้นเพื่อส่งต่อไปยัง Core Layer เลเยอร์นี้ยังทำหน้าที่ควบคุมการเข้าถึงระหว่างเซกเมนต์ของเครือข่าย (เช่น ระหว่าง VLANs) และจัดการการกรองทราฟฟิกโดยใช้การกรองแพ็กเก็ต (Packet Filtering) และ Access Control Lists (ACLs) อุปกรณ์ใน Distribution Layer มักจะเป็น เราเตอร์ (Router) หรือ สวิตช์แบบมัลติเพล็กซ์ (Multilayer Switches) ที่สามารถจัดการทราฟฟิกที่ซับซ้อนได้

3. Core Layer (เลเยอร์หลัก)

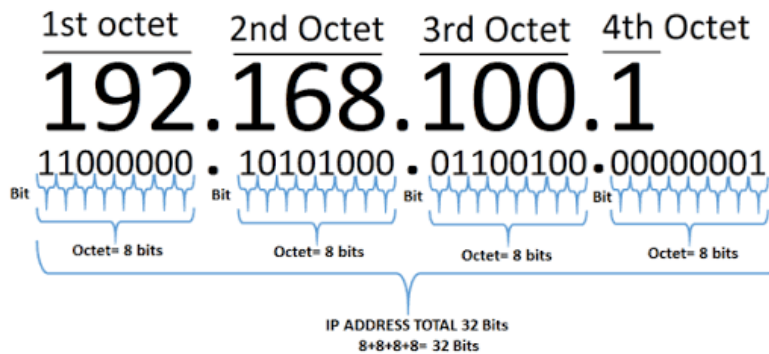
Core Layer เป็นชั้นที่อยู่ด้านบนสุดของเครือข่าย ทำหน้าที่เป็นแกนหลักในการรับและส่งทราฟฟิกที่มาจาก Distribution Layer ไปยังส่วนต่าง ๆ ของเครือข่ายอย่างรวดเร็ว เลเยอร์นี้ต้องมีความเร็วและประสิทธิภาพสูง เพราะทำหน้าที่ในการส่งทราฟฟิกขนาดใหญ่ระหว่างเครือข่ายภายใน (Internal Network) และเครือข่ายภายนอก (External Network) อุปกรณ์ใน Core Layer มักจะเป็น สวิตช์ที่มีความเร็วสูง (High-speed Switches) ที่ออกแบบมาเพื่อรองรับการส่งทราฟฟิกปริมาณมากได้อย่างรวดเร็ว

ความสำคัญของการแยกเลเยอร์

การแบ่งเครือข่ายออกเป็นเลเยอร์ต่าง ๆ ช่วยให้เครือข่ายมีความยืดหยุ่นในการขยายตัวและสามารถจัดการได้ง่ายขึ้น นอกจากนี้ยังช่วยในการจัดการทราฟฟิกอย่างมีประสิทธิภาพ ลดความซับซ้อนในการวินิจฉัยปัญหา และปรับปรุงความปลอดภัยโดยสามารถควบคุมการเข้าถึงในแต่ละเลเยอร์ได้ การเข้าใจโครงสร้างแบบ Access, Distribution และ Core เป็นพื้นฐานสำคัญสำหรับการออกแบบและจัดการเครือข่ายที่มีความซับซ้อนและมีประสิทธิภาพสูง

3.1.3 หมายเลขไอพี (IP Address)

หมายเลขไอพี (Internet Protocol Address) จะแบ่งเป็น 2 รูปแบบที่เป็นมาตรฐานของ IP Address คือ IPv4 (32 บิต) และ IPv6 (128 บิต) โดย IPv4 เป็นรูปแบบที่ใช้งานอย่างแพร่หลายในปัจจุบัน และประกอบด้วยตัวเลข 4 ชุด โดยแต่ละชุดจะมีจุดขึ้น เช่น 192.168.100.1 หรือ 172.16.10.11 เป็นต้น

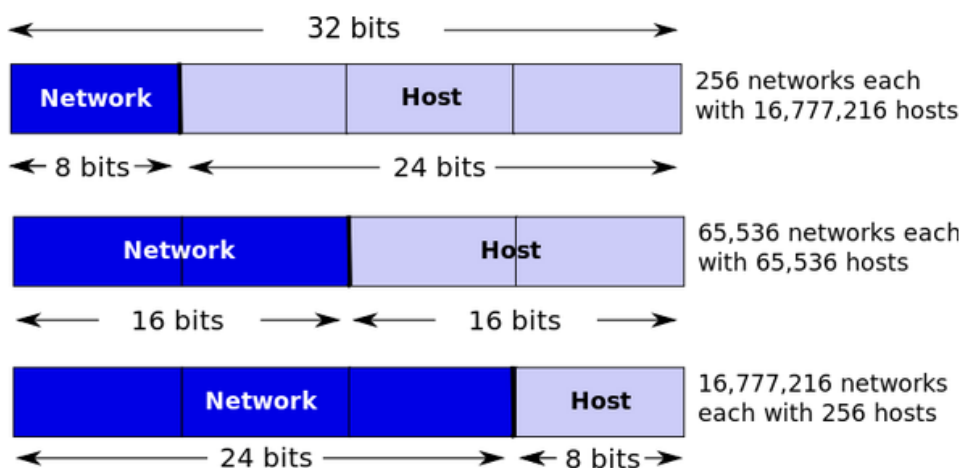


ภาพที่ 3.2 ตัวอย่างรูปแบบของ IP Address

การใช้งาน IPv4 (IP Version 4)

สามารถบอกได้ว่าหมายเลขประจำเครื่องคอมพิวเตอร์แต่ละเครื่องในระบบเครือข่ายที่ใช้ Protocol แบบ TCP/IP ซึ่งหมายเลข IP Address ของเครื่องคอมพิวเตอร์แต่ละเครื่องจะไม่ซ้ำกัน โดยตัวเลข 4 ชุดนี้จะบ่งบอกถึง Network ID กับ Host ID ซึ่งจะบอกให้รู้ว่าเครื่อง Computer ของเราอยู่ในกลุ่ม Network แบบไหนประเภทไหนและเป็นเครื่องไหนใน Network โดยรูปแบบโครงสร้างพื้นฐาน IP Address จะมีดังนี้

- ถ้าส่วนที่เป็น Network เป็นแบบ 8 บิต (1ไบต์) และ Host 24 บิต (3ไบต์) ระบบก็จะแบ่งเป็นเน็ตเวิร์คได้ 256 เน็ตเวิร์ค และแบ่งเป็นโฮสต์ได้ 16,77,216 โฮสต์
- ถ้าส่วนที่เป็น Network เป็นแบบ 16 บิต (2ไบต์) และ Host 16 บิต (2ไบต์) ระบบก็จะแบ่งเป็นเน็ตเวิร์คได้ 65,536 เน็ตเวิร์ค และแบ่งเป็นโฮสต์ได้ 65,536 โฮสต์
- ถ้าส่วนที่เป็น Network เป็นแบบ 24 บิต (3ไบต์) และ Host 8 บิต (1ไบต์) ระบบก็จะแบ่งเป็นเน็ตเวิร์คได้ 16,777,216 เน็ตเวิร์ค และแบ่งเป็นโฮสต์ได้ 256 โฮสต์



ภาพที่ 3.3 รูปแบบโครงสร้างพื้นฐาน IP Address

การแบ่ง Subnet mask ของ IPv4

Subnet mask เป็น Parameter (พารามิเตอร์) อีกตัวหนึ่งที่ต้องระบุควบคู่กับหมายเลข IP Address (ไอพีแอดเดรส) หน้าที่ของ Subnet mask ก็คือ การช่วยในการแยกแยะว่า ส่วนใดภายในหมายเลข IP Address (ไอพี แอดเดรส) เป็น Network Address (เน็ตเวิร์ค แอดเดรส) และส่วนใดเป็นหมายเลข Host Address (โฮสต์ แอดเดรส) ดังนั้น จะสังเกตได้ว่า เมื่อเราระบุ IP Address ให้กับเครื่องคอมพิวเตอร์เราจำเป็นต้องระบุ Subnet mask ลงไปด้วยทุกครั้ง ในการแบ่ง Subnet mask ที่ง่ายที่สุด จะแบ่งในส่วนของ Octet พอดีเป็น /8, /16, /24 ดังตาราง ต่อไปนี้

Prefix length	Subnet Mask in Binary (N=Network, H=Host)	Subnet Mask	#of Subnets	#of hosts
/8	NNNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH 11111111.00000000.00000000.00000000	255.0.0.0	2	16,777,214
/16	NNNNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH 11111111.11111111.00000000.00000000	255.255.0.0	4	65,534
/24	NNNNNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH 11111111.11111111.11111111.00000000	255.255.255.0	8	254

ตารางที่ 3.1 ตารางการแบ่ง Subnet แบบตรง Octet (N=Network, H=Host)

และยังมีการแบ่ง Subnet แบบที่ไม่ตรงกับ Octet จะต้องไปยืมส่วนของ Host ใน Subnet mask มาใช้งาน ดังตารางต่อไปนี้

Prefix length	Subnet Mask in Binary (N=Network, H=Host)	Subnet Mask	#of Subnets	#of hosts
/17	NNNNNNNN.NNNNNNNN.NHHHHHHH.HHHHHHHH 11111111.11111111.10000000.00000000	255.255.128.0	2	32,766
/18	NNNNNNNN.NNNNNNNN.NNHHHHHH.HHHHHHHH 11111111.11111111.11000000.00000000	255.255.192.0	4	16,382
/19	NNNNNNNN.NNNNNNNN.NNNHHHHH.HHHHHHHH 11111111.11111111.11100000.00000000	255.255.224.0	8	8,190
/20	NNNNNNNN.NNNNNNNN.NNNNHHHH.HHHHHHHH 11111111.11111111.11110000.00000000	255.255.240.0	16	4,094
/21	NNNNNNNN.NNNNNNNN.NNNNNHHH.HHHHHHHH 11111111.11111111.11111000.00000000	255.255.248.0	32	2,046
/22	NNNNNNNN.NNNNNNNN.NNNNNHHH.HHHHHHHH 11111111.11111111.11111100.00000000	255.255.252.0	64	1,022
/23	NNNNNNNN.NNNNNNNN.NNNNNNH.HHHHHHHH 11111111.11111111.11111110.00000000	255.255.254.0	128	510
/24	NNNNNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH 11111111.11111111.11111111.00000000	255.255.255.0	256	254
/25	NNNNNNNN.NNNNNNNN.NNNNNNNN.NHHHHHHH 11111111.11111111.11111111.10000000	255.255.255.128	512	126

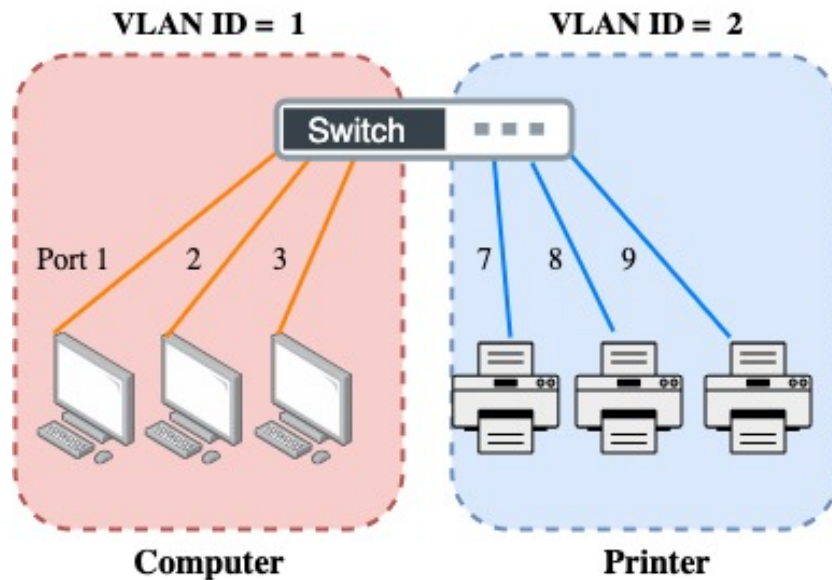
Prefix length	Subnet Mask in Binary (N=Network, H=Host)	Subnet Mask	#of Subnets	#of hosts
/26	NNNNNNNN.NNNNNNNN.NNNNNNNN.NNHHHHHH 11111111.11111111.11111111.11000000	255.255.255.192	1024	62
/27	NNNNNNNN.NNNNNNNN.NNNNNNNN.NNNHHHHH 11111111.11111111.11111111.11100000	255.255.255.224	2048	30
/28	NNNNNNNN.NNNNNNNN.NNNNNNNN.NNNHHHHH 11111111.11111111.11111111.11110000	255.255.255.240	4096	14
/29	NNNNNNNN.NNNNNNNN.NNNNNNNN.NNNHHHHH 11111111.11111111.11111111.11111000	255.255.255.248	8192	6
/30	NNNNNNNN.NNNNNNNN.NNNNNNNN.NNNHHHHH 11111111.11111111.11111111.11111100	255.255.255.252	16384	2

ตารางที่ 3.2 ตารางการแบ่ง Subnet แบบที่ไม่ตรงกับ Octet

3.1.4 VLAN หรือ Virtual Local Area Network

นั่นเป็นคุณสมบัติหนึ่งของ Switch ทำงานอยู่บน Layer2 (Data-Link Layer) โดยหน้าที่หลักของมันคือ การแยกการเชื่อมต่อเครือข่ายคอมพิวเตอร์เป็นส่วน ๆ เป็นการแบ่งกลุ่มของเครื่องคอมพิวเตอร์ปลายทางออกเป็นกลุ่มย่อย ๆ คืออยู่ LAN (แลน) เดียวกัน แต่สามารถสื่อสารกันได้เฉพาะเครื่องในกลุ่มของตนที่อยู่ภายใน VLAN เดียวกันเท่านั้น ตัวอย่างเช่นที่สร้างขึ้นบนเครือข่ายแบบกายภาพ (Physical Network) โดย VLAN จะใช้หมายเลข VLAN (VLAN ID) เป็นตัวกำหนดขอบเขตของเครือข่าย อุปกรณ์ที่อยู่ภายใน VLAN เดียวกันจะสามารถสื่อสารกันได้ แต่ไม่สามารถสื่อสารกับอุปกรณ์ที่อยู่นอก VLAN ได้ และยังมีประโยชน์มากมาย เช่น

1. **ความปลอดภัย:** การแยกข้อมูลที่สำคัญออกจากส่วนอื่นๆ ของเครือข่ายสามารถช่วยป้องกันการเข้าถึงข้อมูลอย่างที่ไม่ได้รับอนุญาตได้
2. **การจัดการเครือข่าย:** VLAN ช่วยให้สามารถจัดการเครือข่ายได้ง่ายขึ้น และสามารถจัดสรรทรัพยากรตามความต้องการของแต่ละส่วน
3. **ลดปัญหาการรบกวน:** เนื่องจากข้อมูลในแต่ละ VLAN จะแยกจากกัน การรบกวนข้อมูลระหว่างกลุ่มต่างๆ ในเครือข่ายจึงลดลง
4. **การใช้ทรัพยากรอย่างมีประสิทธิภาพ:** VLAN ช่วยให้สามารถใช้ทรัพยากรเครือข่ายได้มากขึ้นโดยไม่ต้องเพิ่มอุปกรณ์เครือข่าย เช่น ลดจำนวนการใช้ Switch ลง เนื่องจาก L2 Switch สามารถสร้าง VLAN ได้ถึง 4,095 VLANs (ขึ้นอยู่กับสเปคของ Switch)



ภาพที่ 3.4 รูปการออกแบบ VLAN ภายใน Switch

3.1.5 การจัดการระบบเครือข่ายคอมพิวเตอร์

การจัดการระบบเครือข่ายควรมีเครื่องมือที่สามารถตรวจสอบสถานะเครือข่ายแบบเรียลไทม์ เช่นระบบ Network Monitoring (เช่น PRTG, Zabbix หรือ Nagios) และการตั้งค่าการแจ้งเตือนเมื่อเกิดเหตุผิดปกติ เช่น การล่มของระบบ หรืออุปกรณ์ไม่ตอบสนอง

ผู้ดูแลควรกำหนดแผนการบำรุงรักษาเครือข่ายอย่างสม่ำเสมอ เช่น การอัปเดตเฟิร์มแวร์ของอุปกรณ์เครือข่าย การสำรองค่าการตั้งค่าคอนฟิก และการตรวจสอบ Log File อย่างสม่ำเสมอ รวมถึงมีระบบสำรองข้อมูล (Backup) และแผนการกู้คืน (Recovery Plan) ในกรณีที่เกิดความเสียหาย

3.2 เงื่อนไข/ข้อสังเกต/ข้อควรระวัง/สิ่งที่ควรคำนึงในการปฏิบัติงาน

1. ความปลอดภัยของระบบเป็นสิ่งสำคัญอันดับแรก ควรกำหนดสิทธิ์การเข้าถึงระบบเครือข่ายตามระดับผู้ใช้งาน และไม่ควรเปิดพอร์ตหรือบริการที่ไม่จำเป็นไว้บนเครือข่าย
2. การเปลี่ยนแปลงหรือปรับปรุงระบบควรมีการบันทึก (Documentation) ทุกครั้ง เพื่อให้สามารถติดตามย้อนหลังได้ กรณีเกิดปัญหา หรือมีการเปลี่ยนผู้ดูแลระบบ
3. ไม่ควรกำหนด IP ซ้ำกันในระบบ โดยควรมีระบบจอง IP แบบ Static และจัดทำเอกสารแสดงรายการ IP Address ทั้งหมด
4. ระบบต้องสามารถปรับขยายได้ในอนาคต เช่น หากมีการเพิ่มจำนวนอาคารหรือจุดใช้งาน ควรเผื่อแผนผังและพอร์ตบนอุปกรณ์ให้เพียงพอ

5. สำรองข้อมูลค่าคอนฟิกของอุปกรณ์เครือข่ายไว้อย่างสม่ำเสมอ และเก็บไว้ในที่ปลอดภัย โดยเฉพาะในกรณีที่ต้องเปลี่ยนหรือซ่อมอุปกรณ์
6. การทำงานร่วมกับผู้ใช้ควรสื่อสารให้เข้าใจง่าย เพื่อป้องกันการใช้งานอุปกรณ์เครือข่าย ผิดประเภท เช่น การถอดสายสัญญาณหรือรีเซ็ตอุปกรณ์โดยไม่แจ้งเจ้าหน้าที่
7. อัปเดต Firmware และ Patch ความปลอดภัยของอุปกรณ์อยู่เสมอ เพื่อป้องกันช่องโหว่จากภัยคุกคามทางไซเบอร์
8. ควรทดสอบระบบก่อนเปิดใช้งานจริง ทั้งด้านการเชื่อมต่อ ความเร็ว ความเสถียร และความปลอดภัย รวมถึงการจำลองเหตุการณ์ฉุกเฉิน เช่น การล่มของเซิร์ฟเวอร์หลัก

บทที่ 4

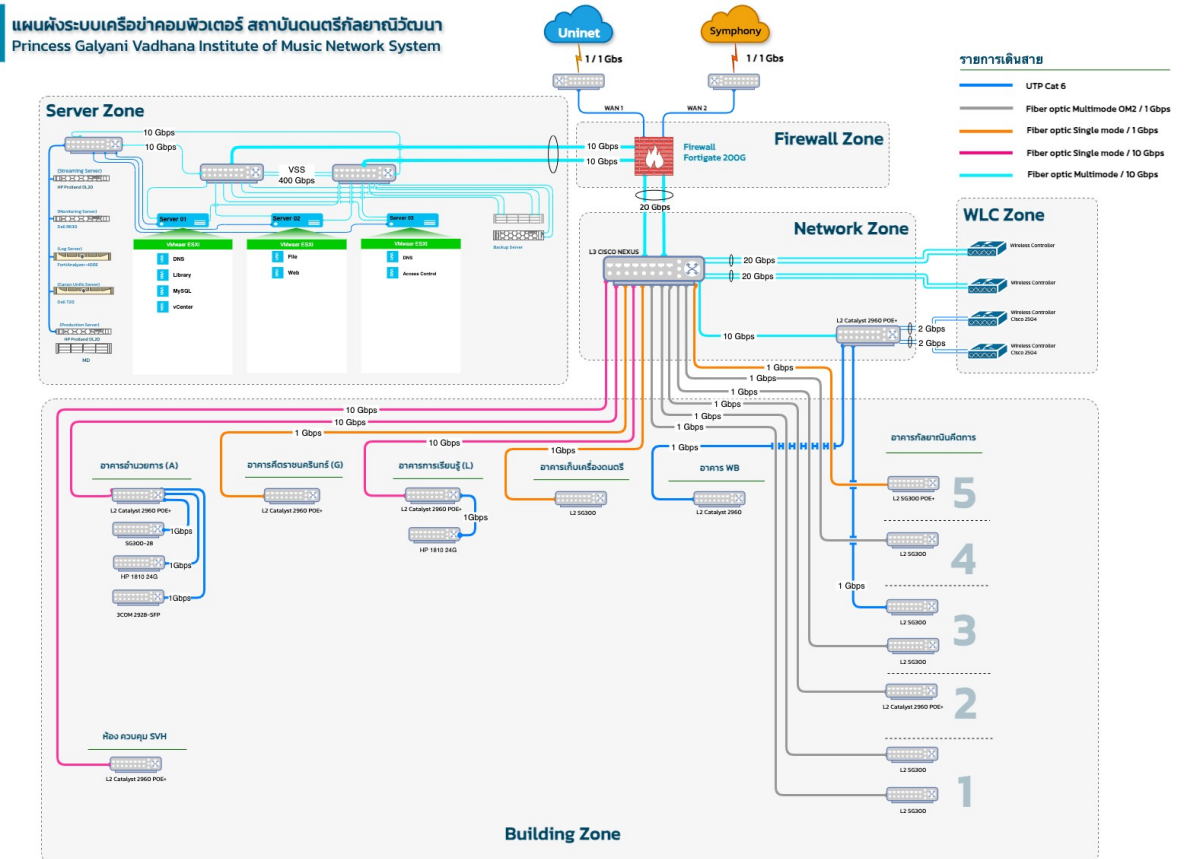
วิธีการปฏิบัติงาน

4.1 กิจกรรมและแผนการปฏิบัติงาน

ในการออกแบบและการจัดการระบบเครือข่ายคอมพิวเตอร์ ของสถาบันดนตรีกัลยาณีวัฒนา ผู้ปฏิบัติงานต้องมีความรู้และความเข้าใจเกี่ยวกับภาพรวมของทั้งระบบ เพื่อให้เข้าใจหลักการทำงาน และสามารถปฏิบัติงานได้อย่างถูกต้อง โดยสิ่งที่จำเป็นต้องเข้าใจก่อนการ ปฏิบัติงานมีดังนี้

- 4.1.1. การออกแบบเครือข่ายลักษณะ 3-Tier Design ในการติดตั้งอุปกรณ์
- 4.1.2. การจัดสรร IP Address เพื่อใช้งานภายในของสถาบันดนตรีกัลยาณีวัฒนา

4.1.1 การออกแบบเครือข่ายลักษณะ 3-Tier Design ในการติดตั้งอุปกรณ์



ภาพที่ 4.1 แผนผังระบบเครือข่ายคอมพิวเตอร์ ของสถาบันดนตรีกัลยาณีวัฒนา

การออกแบบเครือข่ายลักษณะ 3-Tier Design (สถาปัตยกรรมแบบ 3 ชั้น) โดยแบ่งออกเป็นสามชั้นหลักโครงสร้างของเครือข่ายที่แบ่งออกเป็นสามเลเยอร์หลัก ได้แก่ Access Layer, Distribution Layer และ Core Layer ซึ่งเป็นโมเดลการออกแบบเครือข่ายที่ช่วยให้การจัดการเครือข่ายเป็นไปอย่างมีประสิทธิภาพและสามารถขยายได้อย่างง่ายดาย

โครงสร้างระดับ Core Layer อุปกรณ์ทั้งหมดติดตั้งอยู่ที่ Data Center ที่ทำงานร่วมกับ Firewall, Router, เครื่องคอมพิวเตอร์แม่ข่ายระบบต่างๆและยังเป็นจุดเชื่อมต่อกับผู้ให้บริการอินเทอร์เน็ตเพื่อรับส่งข้อมูลสู่อินเทอร์เน็ตอีกด้วย

โครงสร้างระดับ Distribution Layer อุปกรณ์ในส่วนนี้จะถูกติดตั้งที่ Building Zone มีการเชื่อมต่อด้วยสายใยแก้วนำแสงไปยังอุปกรณ์ เพื่อรองรับการเชื่อมต่อจากอุปกรณ์ในระดับ Access Layer ที่ติดตั้งตามอาคารนั้น ๆ โดยได้ดังนี้

1. อาคารอำนวยการ
2. อาคารคิตราชนครินทร์
3. อาคารกัลยาณินคีตการ
4. อาคารศูนย์การเรียนรู้และสหนาการ
5. อาคารเก็บเครื่องดนตรี
6. อาคารศูนย์เรียนรู้ดนตรีไทย - เอเชีย (Wood Box)

โครงสร้างระดับ Access Layer จะเป็นเลเยอร์ที่ใกล้ชิดติดกับผู้ใช้มากที่สุดเป็นจุดที่นำเครื่องคอมพิวเตอร์ของผู้ใช้เข้าสู่ระบบเครือข่าย สำหรับ LAN อุปกรณ์ที่ทำงานอยู่ในเลเยอร์นี้มักเป็นสวิตช์เลเยอร์ 2 จะถูกเชื่อมโยงขึ้นไปยังสวิตช์ที่อยู่ในระดับ Distribution Layer ด้วยสาย UTP (Cat 6) สวิตช์ที่ว่านี้จำเป็นต้องมีพอร์ต UPLINK โดยทำหน้าที่เชื่อมต่ออุปกรณ์ปลายทางเข้ากับเครือข่ายหลักไปยังอุปกรณ์ต่าง ๆ เช่น เครื่องคอมพิวเตอร์, เครื่องปริ้นเตอร์, เครื่องสแกนเอกสาร และอุปกรณ์ต่าง ๆ เป็นต้น

4.1.2 การจัดสรรหมายเลข IP Address เพื่อใช้งานภายในสถาบัน

งานเทคโนโลยีและสารสนเทศมีหน้าที่รับผิดชอบกำหนดหมายเลข IP Address เพื่อนำไปใช้งานภายในระบบเครือข่ายของสถาบันดนตรีกัลยาณินวัฒนา โดยจัดสรรหมายเลข IP Address อย่างเป็นระบบจะช่วยให้ใช้งานระบบเครือข่ายได้อย่างเต็มที่ และผู้ดูแลระบบสามารถดูแลระบบได้อย่างราบรื่นโดยจะได้รับการจัดสรรหมายเลข IPv4 Address จำนวน 2 ชุด ได้แก่

Public IP Address (หมายเลขไอพีสาธารณะ) เป็นหมายเลข IP Address สาธารณะที่นำไปใช้งานเพื่อให้สามารถใช้บริการจากภายนอกระบบเครือข่ายของทางสถาบันดนตรีกัลยาณินวัฒนา เช่น Internet และผู้ใช้งานภายนอกสามารถเรียกหาอุปกรณ์ภายในเพื่อขอใช้บริการได้ โดยทางงาน

เทคโนโลยีและสารสนเทศจะจัดสรรให้หน่วยงานที่มีความจำเป็นที่จะต้องใช้งาน โดยได้รับการอนุมัติจากผู้บริหารสถาบัน

Private IP Address (หมายเลขไอพีส่วนตัว) เป็นหมายเลข IP Address ที่สงวนให้ใช้ภายในสถาบันดนตรีกัลยาณีวัฒนา โดยการเรียกใช้งานจากภายนอกไม่สามารถทำได้และมีความปลอดภัยสูงกว่า เนื่องจากไม่สามารถเข้าถึงจากอินเทอร์เน็ตภายนอกได้โดยตรง

หลักการจัดสรรหมายเลข Private IP Address (หมายเลขไอพีส่วนตัว) เพื่อใช้ภายในระบบเครือข่ายของทางสถาบันดนตรีกัลยาณีวัฒนา

เนื่องจาก Public IP Address (หมายเลขไอพีสาธารณะ) มีจำนวนจำกัด และไม่เหมาะสมสำหรับนำมาใช้ภายในระบบเครือข่ายภายในสถาบันดนตรีกัลยาณีวัฒนา จึงนำ Private IP Address (หมายเลขไอพีส่วนตัว) มาใช้งานภายในสถาบันดนตรีกัลยาณีวัฒนา จึงมีการจัดสรรการใช้งานในส่วนต่าง ๆ ให้ครอบคลุม ผู้ดูแลระบบจึงต้องมีความเข้าใจถึงหลักการจัดสรร IP Address ที่ใช้อยู่ในปัจจุบัน เพื่อให้สอดคล้องกับการติดตั้งอุปกรณ์ระบบเครือข่ายภายในสถาบันดนตรีกัลยาณีวัฒนา โดยการจัดสรรหมายเลข IP Address จึงอ้างอิงการแบ่งกลุ่มของเครื่องคอมพิวเตอร์ โดย VLAN จะใช้หมายเลข VLAN (VLAN ID) เป็นตัวกำหนดขอบเขตของเครือข่ายของการติดตั้งอุปกรณ์ และใช้ Private IP Address 10.0.0.0/8 ใช้สำหรับจัดสรรในหน่วยงานต่าง ๆ และบริการของส่วนกลาง เพื่อให้การดูแลและแก้ไขปัญหาเป็นไปในแนวทางเดียวกัน

VLANID	Subnet	รายละเอียด
VLAN 10	192.168.10.0 /24	สำหรับการให้บริการ อาคารอำนวยการ
VLAN 20	192.168.20.0 /24	สำหรับการให้บริการ อาคารคีตราชนครินทร์
VLAN 30	192.168.30.0 /24	สำหรับการให้บริการ อาคารกัลยาณินคิดการ และอาคารศูนย์เรียนรู้ดนตรีไทย - เอเชีย (Wood Box)
VLAN 40	192.168.40.0 /24	สำหรับการให้บริการ อาคารศูนย์การเรียนรู้และสันนทนาการ
VLAN 50	192.168.50.0 /24	สำหรับการให้บริการ อาคารเก็บเครื่องดนตรี

ตารางที่ 4.1 การใช้หมายเลขไอพีแอดเดรส รุ่น4 (IPv4) แบบ Private Network สำหรับกำหนดให้แก่อุปกรณ์คอมพิวเตอร์สำหรับผู้ใช้งานใน Building Zone

จากตารางที่ 4.1 จะเป็นการกำหนดหมายเลขไอพีแอดเดรสเพื่อให้บริการคอมพิวเตอร์สำหรับการให้บริการอาคารต่าง ๆ เพื่อให้สามารถตรวจสอบผู้ใช้งานอุปกรณ์คอมพิวเตอร์ได้รับหมายเลขไอพีแอดเดรส ที่ใช้งานมาจากอาคารไหนและใครเป็นผู้ใช้งาน

VLAN	Subnet	รายละเอียด
VLAN 98	192.168.98.0 /24	สำหรับการให้บริการ อุปกรณ์ประจำเครื่อง Access Point (แอคเซสพอยต์) ที่เชื่อมต่อกับ WLC Cisco XXXXXX
VLAN 97	192.168.97.0 /24	สำหรับการให้บริการ อุปกรณ์ประจำเครื่อง Access Point (แอคเซสพอยต์) ที่เชื่อมต่อกับ WLC Cisco 2504
VLAN 6	192.168.6.0 /23	สำหรับการให้บริการสัญญาณอินเทอร์เน็ตไร้สาย PGVIN_WiFi
VLAN 9	192.168.9.0 /24	สำหรับการให้บริการสัญญาณอินเทอร์เน็ตไร้สาย PGVIN_IoT_WiFi

ตารางที่ 4.2 การใช้หมายเลขไอพีแอดเดรส รุ่น4 (IPv4) แบบ Private Network สำหรับกำหนดให้แก่อุปกรณ์ Access Point (แอคเซสพอยต์) ใน WIFI Zone

VLANID	Subnet	รายละเอียด
VLAN 99	192.168.99.0 /24	สำหรับการให้บริการ - อาคารอำนวยการ - อาคารคิตราชนครินทร์ - อาคารกัลยาณินคิตราการ - อาคารศูนย์การเรียนรู้และสหนาการ - อาคารเก็บเครื่องดนตรี - อาคารศูนย์เรียนรู้ดนตรีไทย - เอเชีย (Wood Box)

ตารางที่ 4.3 การใช้หมายเลขไอพีแอดเดรส รุ่น4 (IPv4) แบบ Private Network สำหรับกำหนดให้แก่อุปกรณ์ Network Switch ประจำ Building Zone

VLANID	Subnet	รายละเอียด
VLAN 100	192.168.100.0 /24	สำหรับการให้บริการอุปกรณ์ Network ที่ทำการติดตั้งภายในห้อง Data Center

ตารางที่ 4.4 การใช้หมายเลขไอพีแอดเดรส รุ่น4 (IPv4) แบบ Private Network สำหรับกำหนดให้แก่อุปกรณ์ Network ที่ทำการติดตั้งภายในห้อง Data Center

VLANID	Subnet	รายละเอียด
VLAN 110	192.168.110.0 /24	สำหรับเครื่องคอมพิวเตอร์ Server ในกลุ่ม Web Server, ERP Server เป็นต้น
VLAN 111	192.168.111.0 /24	สำหรับเครื่องคอมพิวเตอร์ Server ในกลุ่ม การจัดการ เช่น Log Server, Network Monitoring เป็นต้น

ตารางที่ 4.5 การใช้หมายเลขไอพีแอดเดรส รุ่น4 (IPv4) แบบ Private Network สำหรับกำหนดให้แก่อุปกรณ์คอมพิวเตอร์ Server ประจำ Server Zone

VLANID	Subnet	รายละเอียด
VLAN 201	192.168.201.0 /24	สำหรับ ระบบ VPN ที่เข้ามาในช่องทาง WAN 1
VLAN 202	192.168.202.0 /24	สำหรับ ระบบ VPN ที่เข้ามาในช่องทาง WAN 2

ตารางที่ 4.6 การใช้หมายเลขไอพีแอดเดรส รุ่น4 (IPv4) แบบ Private Network สำหรับกำหนดให้แก่ระบบ VPN (Virtual Private Network)

VLANID	Subnet	รายละเอียด
VLAN 2	192.168.2.0 /24	ระบบกล้องวงจรปิด (ทุกตึก)
VLAN 3	192.168.3.0 /24	ระบบประตูอิเล็กทรอนิกส์, และเครื่องลงเวลาเข้าออก
VLAN 4	192.168.4.0 /24	ระบบโทรศัพท์

ตารางที่ 4.7 การใช้หมายเลขไอพีแอดเดรส รุ่น4 (IPv4) แบบ Private Network สำหรับกำหนดให้แก่อุปกรณ์อื่น ๆ

แผนการปฏิบัติงาน

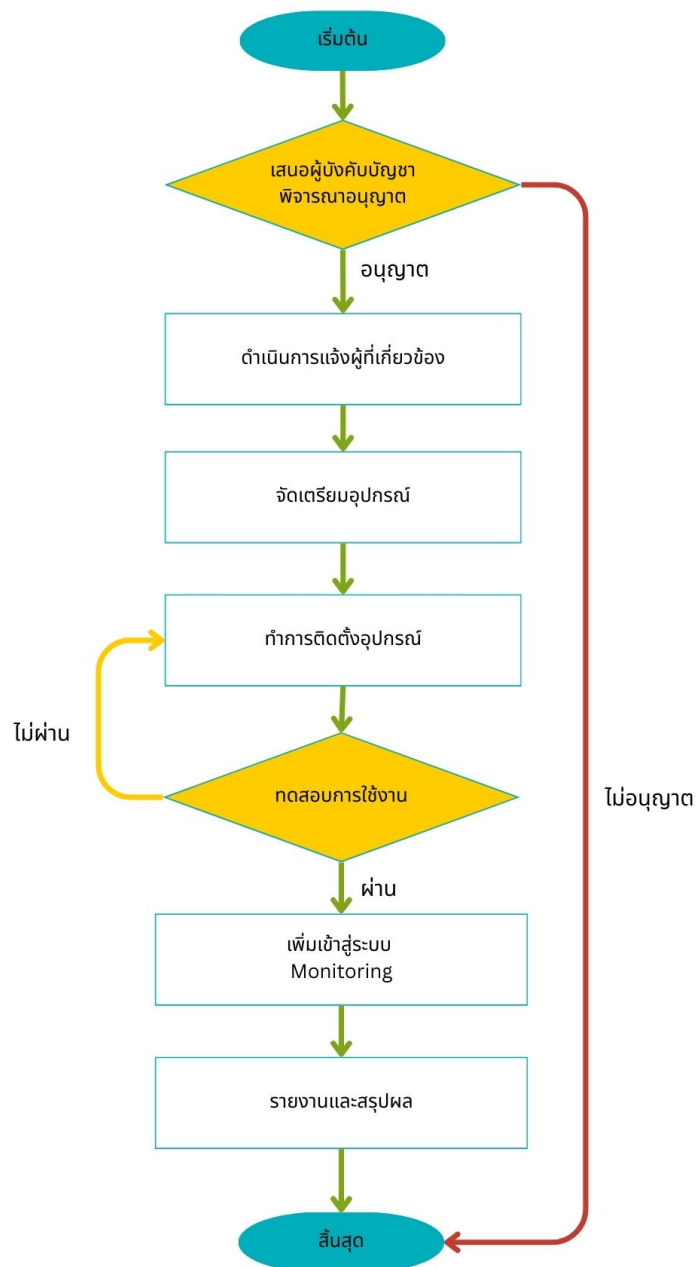
ลำดับ	กิจกรรมการปฏิบัติงาน	ระยะเวลาดำเนินงาน (วันทำการ)	วิธีการปฏิบัติงาน
1	เสนอผู้บังคับบัญชา พิจารณาอนุญาต	3-5 วัน	- จัดทำบันทึกข้อความ/โครงการ - ส่งเอกสารผ่านระบบสารบรรณ - รอการอนุมัติจากผู้บริหาร
2	ดำเนินการแจ้งผู้ที่เกี่ยวข้อง	1-2 วัน	- แจ้งกำหนดการและรายละเอียดการติดตั้ง - ประสานกับหน่วยงานและผู้ใช้ที่ได้รับผลกระทบโดยตรง
3	จัดเตรียมอุปกรณ์	2-3 วัน	- ตรวจสอบรายการอุปกรณ์ - ตั้งค่าเบื้องต้น เช่น IP Address, VLAN - ตรวจสอบสายและอุปกรณ์เสริม
4	ทำการติดตั้งอุปกรณ์	5-7 วัน	- เดินสายสัญญาณ - ติดตั้ง Switch ตามตำแหน่ง ปรับปรุงค่าคอนฟิก - ตรวจสอบการเชื่อมต่อกับ Core Switch
5	ทดสอบการใช้งาน	1 วัน	- ทดสอบการเชื่อมต่อ LAN / Wi-Fi - ตรวจสอบ VLAN, IP และ Gateway - ตรวจสอบความเร็ว Bandwidth และ ความเสถียร
	หากไม่ผ่าน ให้แก้ไข แล้วทดสอบใหม่	3-5 วัน	- ปรับปรุงค่าคอนฟิก - เปลี่ยนอุปกรณ์หากจำเป็น - ทดสอบซ้ำจนกว่าจะผ่านตามมาตรฐาน
6	เพิ่มเข้าสู่ระบบ Monitoring	1 วัน	- เพิ่มอุปกรณ์เข้าระบบ Monitoring - ตั้งค่าแจ้งเตือน Real-time - บันทึก Log การทำงาน
7	รายงานและสรุปผล	1 วัน	- จัดทำรายงานสรุปผลการติดตั้งและการ ทดสอบ - เสนอผู้บังคับบัญชา

ตารางที่ 4.8 ตารางแผนการปฏิบัติงาน

4.2 ขั้นตอนในการปฏิบัติงาน

ตามที่ได้ทำการออกแบบ Vlan แต่ละโซนแล้ว ก็จะได้ชุดของ IP Address ในการบริหารจัดการเพื่อให้สอดคล้องกับการติดตั้งอุปกรณ์ระบบเครือข่ายภายในสถาบันดนตรีกัลยาณีวัฒนาสามารถแบ่งแนวทางในการปฏิบัติงาน ได้แก่

1) การติดตั้งเพิ่มเติมหรือปรับปรุงระบบตามงบประมาณที่ได้รับโดยมีขั้นตอนการปฏิบัติงานสามารถอธิบายในรูปแบบของ Activity Diagram ได้ดังนี้




ภาพที่ 4.2 แผนผังขั้นตอนการปฏิบัติงาน

4.3 วิธีปฏิบัติงาน

จากภาพที่ 4.2 สามารถอธิบายขั้นตอนการทำงานได้ดังนี้

ขั้นตอนที่ 1 ขั้นตอนการนำเสนอผู้บังคับบัญชาพิจารณาอนุญาต ก่อนที่จะทำการติดตั้งจำเป็นต้องแจ้งผู้บังคับบัญชาถึงความจำเป็นที่จะต้องทำการติดตั้งอุปกรณ์เพิ่มเติมหรือทำการเปลี่ยนอุปกรณ์และบอกช่วงเวลาทำการติดตั้งเพื่อลดผลกระทบจากการไม่สามารถใช้งานระบบได้ ให้ เป็นลายลักษณ์อักษรผ่านระบบสารบัญัติอิเล็กทรอนิกส์ โดยแบ่งเป็น 2 ทางเลือก คือ พิจารณาอนุญาต หรือไม่อนุญาตให้ดำเนินการ ในกรณีที่อนุญาตให้ดำเนินการตามขั้นตอนต่อไปและไม่อนุญาตให้ดำเนินการก็ให้หยุดการดำเนินงาน



บันทึกข้อความ

ส่วนราชการ สถาบันเทคโนโลยีนานาชาติสิรินธร โทร 0 2447 8597 โทรสาร 0 2447 8598
ที่ อธ8501/2568 วันที่ 16 มิถุนายน 2568

เรื่อง ขออนุมัติปรับปรุงระบบเครือข่ายคอมพิวเตอร์ เพื่อเปลี่ยนอุปกรณ์รักษาความปลอดภัย (Next Generation Firewall) สถาบันเทคโนโลยีนานาชาติสิรินธร

เรียน อธิการบดี

ตามที่ สถาบันเทคโนโลยีนานาชาติสิรินธร ได้มีการจัดซื้อครุภัณฑ์ ชุดอุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) และชุดอุปกรณ์กระจายสัญญาณไร้สาย สถาบันเทคโนโลยีนานาชาติสิรินธร ทั้งนี้ จึงมีความจำเป็นต้องทำการเปิดระบบปิดปรับปรุงระบบเครือข่ายคอมพิวเตอร์ของสถาบันเทคโนโลยีนานาชาติสิรินธร เพื่อปรับปรุงระบบเครือข่ายคอมพิวเตอร์ของสถาบันเทคโนโลยีนานาชาติสิรินธร ให้มีประสิทธิภาพรับ-ส่ง ของสัญญาณอินเทอร์เน็ตให้ดีขึ้น ในวันที่ 14 มิถุนายน พ.ศ.2568 ตั้งแต่เวลา 17.00 น. เป็นต้นไป) ส่งผลให้ในวันดังกล่าวจะไม่สามารถเข้าใช้งานระบบเครือข่ายคอมพิวเตอร์ สถาบันเทคโนโลยีนานาชาติสิรินธรได้

จึงเรียนเพื่อไม่พิจารณาอนุมัติปิดปรับปรุงระบบเครือข่ายคอมพิวเตอร์ เพื่อเปลี่ยนอุปกรณ์รักษาความปลอดภัย (Next Generation Firewall) สถาบันเทคโนโลยีนานาชาติสิรินธรขอพระคุณด้วย

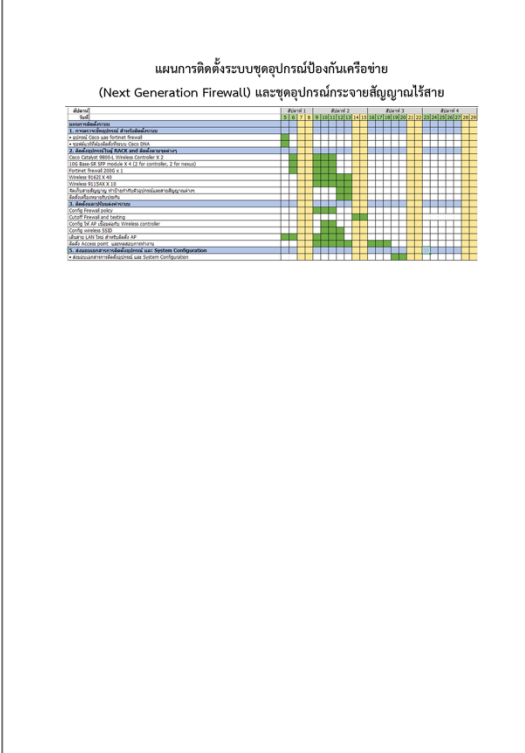
นายทศกร ศรีวิเศษ
(นายทศกร ศรีวิเศษ)
นักเทคโนโลยีคอมพิวเตอร์

เนื่องจากคณบดีทางบริษัทได้ดำเนินการเข้ามาติดตั้ง
และมีการประชุมหารือด้วยกันแล้ว
จึงเลือกเวลาในวันและเวลาที่กระทบกับกิจกรรมอันน้อยที่สุด
จึงเรียนมาเพื่อพิจารณาครับ

ผู้รักษาการแทนอธิการบดี

อนุมัติ

ศาสตราจารย์พิเศษ
ผู้รักษาการแทนอธิการบดี



**แผนการติดตั้งระบบชุดอุปกรณ์ป้องกันเครือข่าย
(Next Generation Firewall) และชุดอุปกรณ์กระจายสัญญาณไร้สาย**

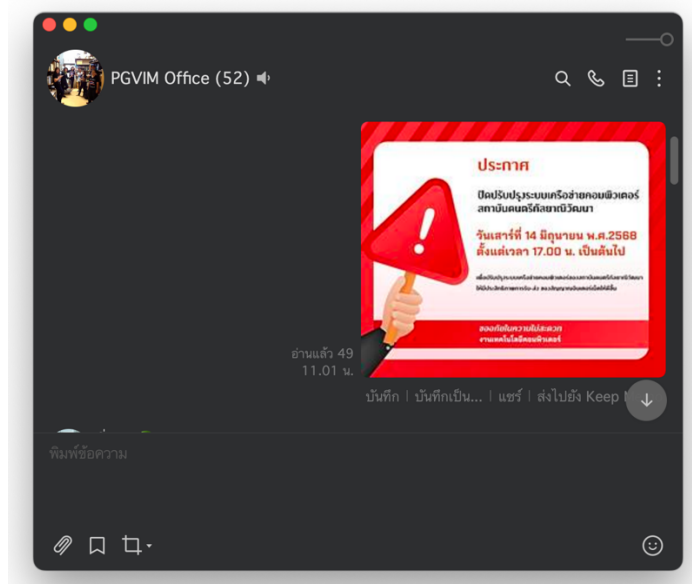
Activity	April 1	April 2	April 3	April 4
1. ติดตั้งและทดสอบระบบ	Completed	Completed	Completed	Completed
2. ตรวจสอบและทดสอบระบบ	Completed	Completed	Completed	Completed
3. ปิดระบบเครือข่าย	Completed	Completed	Completed	Completed
4. ตรวจสอบและทดสอบระบบ	Completed	Completed	Completed	Completed
5. เปิดระบบเครือข่าย	Completed	Completed	Completed	Completed
6. ตรวจสอบและทดสอบระบบ	Completed	Completed	Completed	Completed
7. ปิดระบบเครือข่าย	Completed	Completed	Completed	Completed
8. ตรวจสอบและทดสอบระบบ	Completed	Completed	Completed	Completed
9. เปิดระบบเครือข่าย	Completed	Completed	Completed	Completed
10. ตรวจสอบและทดสอบระบบ	Completed	Completed	Completed	Completed
11. ปิดระบบเครือข่าย	Completed	Completed	Completed	Completed
12. ตรวจสอบและทดสอบระบบ	Completed	Completed	Completed	Completed
13. เปิดระบบเครือข่าย	Completed	Completed	Completed	Completed
14. ตรวจสอบและทดสอบระบบ	Completed	Completed	Completed	Completed
15. ปิดระบบเครือข่าย	Completed	Completed	Completed	Completed
16. ตรวจสอบและทดสอบระบบ	Completed	Completed	Completed	Completed
17. เปิดระบบเครือข่าย	Completed	Completed	Completed	Completed
18. ตรวจสอบและทดสอบระบบ	Completed	Completed	Completed	Completed
19. ปิดระบบเครือข่าย	Completed	Completed	Completed	Completed
20. ตรวจสอบและทดสอบระบบ	Completed	Completed	Completed	Completed
21. เปิดระบบเครือข่าย	Completed	Completed	Completed	Completed
22. ตรวจสอบและทดสอบระบบ	Completed	Completed	Completed	Completed
23. ปิดระบบเครือข่าย	Completed	Completed	Completed	Completed
24. ตรวจสอบและทดสอบระบบ	Completed	Completed	Completed	Completed
25. เปิดระบบเครือข่าย	Completed	Completed	Completed	Completed
26. ตรวจสอบและทดสอบระบบ	Completed	Completed	Completed	Completed
27. ปิดระบบเครือข่าย	Completed	Completed	Completed	Completed
28. ตรวจสอบและทดสอบระบบ	Completed	Completed	Completed	Completed
29. เปิดระบบเครือข่าย	Completed	Completed	Completed	Completed
30. ตรวจสอบและทดสอบระบบ	Completed	Completed	Completed	Completed

ภาพที่ 4.3 ตัวอย่างบันทึกข้อความ ขออนุมัติปิดปรับปรุงระบบเครือข่ายคอมพิวเตอร์และแผนการติดตั้ง

ขั้นตอนที่ 2 การดำเนินการแจ้งผู้ที่เกี่ยวข้อง หลังจากได้รับการอนุญาตให้ดำเนินการติดตั้ง ให้ทำการแจ้งประกาศปิดระบบให้ผู้ใช้งานทราบก่อนสำหรับหน่วยงานที่ได้รับผลกระทบ โดยแจ้งข้อความผ่านระบบสื่อสารภายในสถาบัน เช่น Line กลุ่มของสถาบันและทำแจ้งล่วงหน้า 1-2 วัน ก่อนทำการติดตั้ง พร้อมทั้งอธิบายเหตุผล และบอกถึงช่วงเวลาทำการ เพื่อให้หน่วยงานที่ได้รับผลกระทบได้ทำการวางแผนในการทำงานในช่วงเวลาที่ทำการติดตั้งอุปกรณ์เพิ่มเติมหรือทำการเปลี่ยนอุปกรณ์นั้น



ภาพที่ 4.4 ประกาศปิดปรับปรุงระบบเครือข่ายคอมพิวเตอร์สถาบันดนตรีกลายาณวิวัฒนา



ภาพที่ 4.5 การแจ้งประกาศปิดปรับปรุงระบบเครือข่ายคอมพิวเตอร์ บน Application Line

ขั้นตอนที่ 3 ก่อนที่จะทำการติดตั้งจะต้องจัดเตรียมเครื่องมือติดตั้งให้พร้อม เช่น ไขควง, น็อต ยึดแร็ค, กุญแจตู้แร็ค, หูช้างสำหรับติดยึดตู้แร็ค, คีมตัดและเข้าหัวสายแลน, อุปกรณ์จัดสาย, สาย Console ต่าง ๆ และ คอมพิวเตอร์ สำหรับในการตั้งค่า เป็นต้น



ไขควง



น็อตยึดแร็ค



หูช้างสำหรับติดยึดตู้แร็ค



กุญแจตู้แร็ค



คีมตัดและเข้าหัวสายแลน



อุปกรณ์จัดสาย



สาย Console
USB to Serial Port (DB9)



สาย Console
USB to RJ45



สาย Console Serial Port (DB9)
Female To Female



คอมพิวเตอร์แล็ปท็อป

ภาพที่ 4.6 ชุดเครื่องมือเบื้องต้นสำหรับ ติดตั้งสำหรับอุปกรณ์สวิตช์ (Switch)

ขั้นตอนที่ 4 การทำการติดตั้งอุปกรณ์ ผู้ปฏิบัติงานต้องนำอุปกรณ์ที่จะติดตั้ง มาตั้งค่าการทำงาน (Configuration) ตามที่ออกแบบตามหลักการทฤษฎีและมาตรฐานที่เกี่ยวข้องกับระบบเครือข่าย และการจัดสรรหมายเลข IP Address เพื่อใช้งานภายในสถาบัน หลังจากได้เตรียมข้อมูลต่าง ๆ แล้ว ก่อนที่จะนำอุปกรณ์ไปติดตั้ง ผู้ปฏิบัติงานต้องพิจารณาความต้องการของหน่วยงานดังนี้

1. การเชื่อมต่อไปยังหน่วยงาน ใช้ port ชนิดใด UTP หรือ โยแก้วนำแสง
2. มีการเชื่อมต่อบริการต่าง ๆ ของสถาบัน ด้วย port ชนิดใด
3. Port ที่เชื่อมต่อใช้ความเร็วเท่าใด 1 Gbps หรือ 10 Gbps
4. มีรูปแบบการเชื่อมต่อเข้ากับหน่วยงานแบบใด ต่อเข้ากับอุปกรณ์ Switch หรือ Firewall
5. หมายเลข IP Address ที่ต้องใช้งานกับหน่วยงาน ทั้ง Private IP Address และ Public IP Address

เพื่อให้สามารถทำงานได้ อย่างเหมาะสมตามต้องการ และสามารถดูแลด้วยการมอนิเตอร์หรือเข้าถึงจากระยะไกลต่อไปหลังจากติดตั้งไปแล้ว มีวิธีการดังนี้

การเข้าถึงอุปกรณ์เพื่อ Configuration

อุปกรณ์ที่นำมาใช้ในระบบเครือข่ายนั้น เป็นอุปกรณ์ที่อยู่ในระดับสูงจึงต้องมีการตั้งค่าก่อนใช้งานทุกครั้ง เพื่อให้สามารถทำงานเข้ากับระบบที่มีอยู่ได้ และทำให้ทำงานได้อย่างถูกต้อง ในการตั้งค่า Configuration มีวิธีการดังนี้

คอนโซล (Console) เป็นการตั้งค่าโดยการเข้าถึงที่ตัวอุปกรณ์ ด้วยการใช้สายคอนโซล (Console) เชื่อมต่อที่ Port ที่แยกจากการใช้งาน โดย Port สำหรับการคอนโซล (Console) จะใช้เพื่อการเข้าถึงอุปกรณ์เพื่อตั้งค่าเท่านั้น สำหรับการใช้คอนโซล (Console) นั้นจะใช้ตอนเริ่มต้นตั้งค่าการใช้งานอุปกรณ์หรือในกรณีที่ไม่สามารถใช้งานจากระยะไกลได้ สายเคเบิลคอนโซล USB to Serial Port (DB9) และ USB to RJ45 ยังรองรับการเชื่อมต่อคอนโซล แต่เฉพาะในกรณีที่สวิตช์ มีพอร์ตคอนโซล RJ45 มีลักษณะคล้ายกับพอร์ตอีเทอร์เน็ตและมีป้ายกำกับว่า CONSOLE ที่ด้านหลังหรือด้านหน้าของสวิตช์

Console Port แบบ RJ45

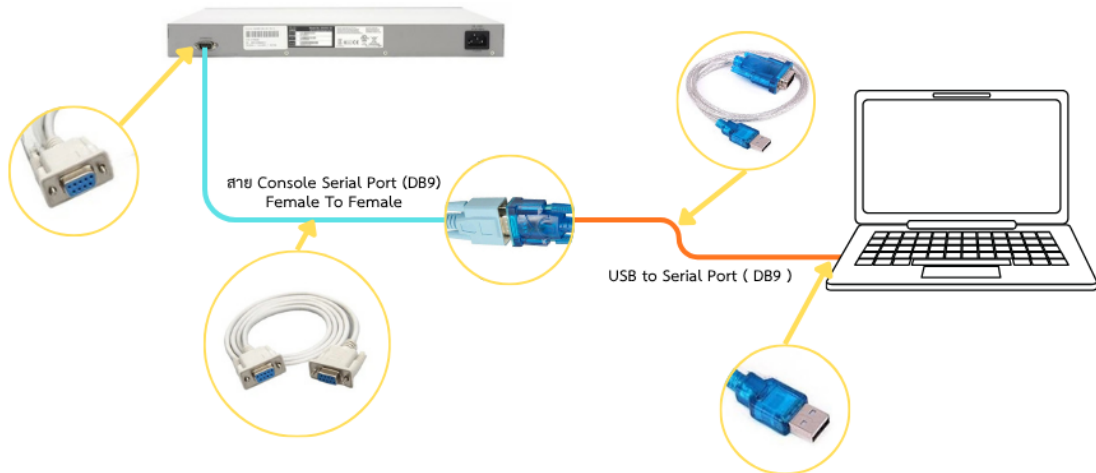


Console Port แบบ Serial Port (DB9)

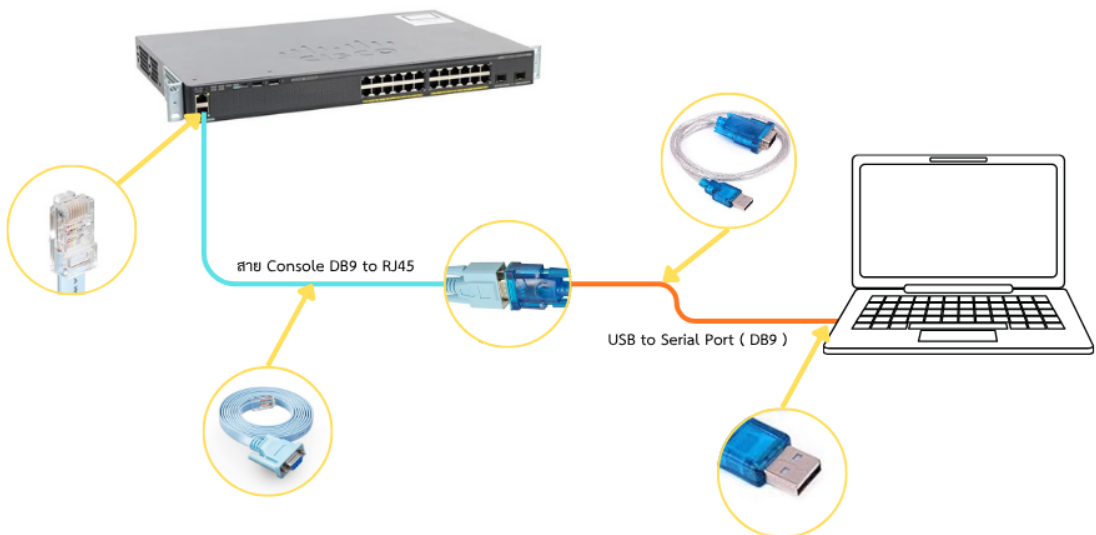


ภาพที่ 4.7 ภาพแสดง Console Port แบบต่าง ๆ บนอุปกรณ์สวิตช์

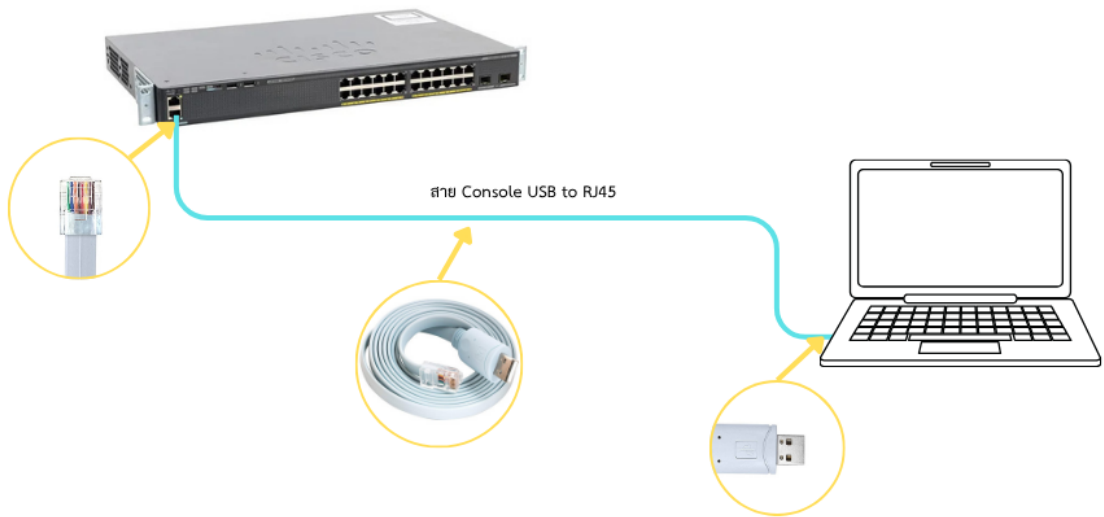
ดังนั้น คอมพิวเตอร์แล็ปท็อปรุ่นใหม่ไม่มี Serial Port (DB9) จึงใช้วิธีการต่อผ่าน USB ตามการใช้งานดังรูป



ภาพที่ 4.8 ภาพแสดงการต่อสาย Console USB to DB 9 (Serial Port) เชื่อมต่อกับ สาย Serial Port (DB9) Female To Female

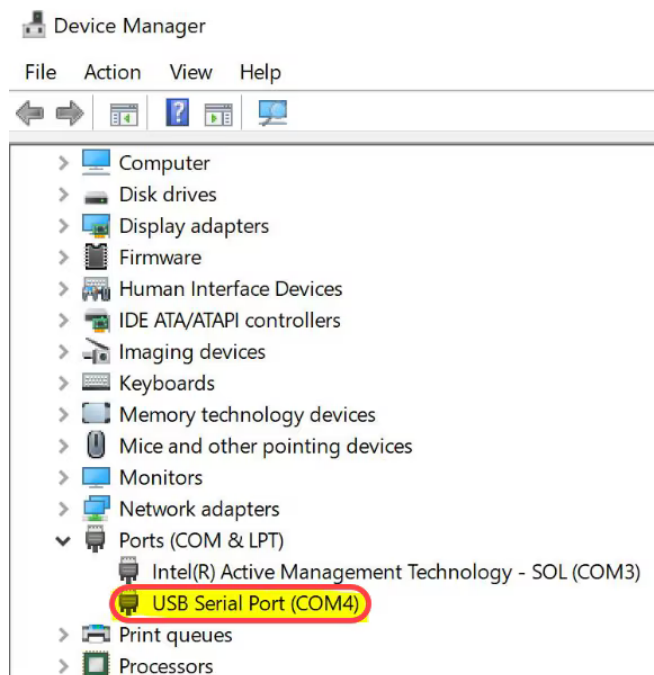


ภาพที่ 4.9 ภาพแสดงการกำหนดหมายเลขพอร์ตเมื่อต่อสาย Console USB to DB 9 (Serial Port) เชื่อมต่อกับ สาย Serial Port (DB9) To RJ45



ภาพที่ 4.10 ภาพแสดงการกำหนดหมายเลขพอร์ตเมื่อต่อสาย Console USB To RJ45

เมื่อคอมพิวเตอร์ทำการเชื่อมต่อด้วยสาย Console USB คอมพิวเตอร์จะกำหนดหมายเลขพอร์ต COM Port ดังภาพที่ 4.11

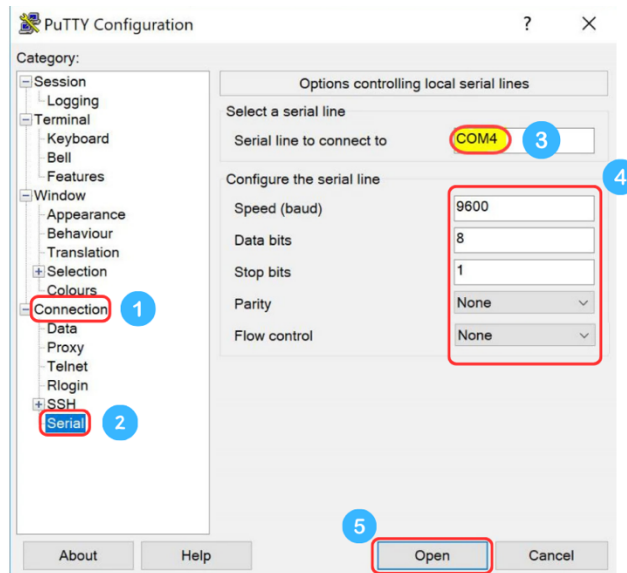


ภาพที่ 4.11 ภาพแสดงการกำหนดหมายเลขพอร์ตเมื่อต่อสาย Console USB

ในกรณีนี้ จะต้องใช้ COM4 Port สำหรับทำการเชื่อมต่อโดยจะแสดงวิธีการเชื่อมต่อคอนโซล (Console) ผ่านโปรแกรม PuTTY มีดังนี้

ขั้นตอนที่ 1. ทำการเชื่อมต่อสวิตช์เข้ากับคอมพิวเตอร์โดยใช้สายเชื่อมต่อคอนโซล (Console) ตามแต่ละสวิตช์มีพอร์ตคอนโซล

ขั้นตอนที่ 2. หลังจากนั้น เปิดแอปพลิเคชัน PuTTY ไปที่ เมนู Connection แล้วเลือกเชื่อมต่อแบบ Serial หน้าต่างการกำหนดค่า PuTTY จะเปิดขึ้นและให้ตั้งค่าตามภาพ



ภาพที่ 4.12 ภาพแสดงหน้าต่าง Application PuTTY ที่เชื่อมต่อแบบ Console USB

ขั้นตอนที่ 3. คลิก Open หน้าต่างคอนโซล COM4 – PuTTY จะเปิดขึ้น แล้วกด Enter บนแป้นพิมพ์เพื่อเปิดใช้งานอินเทอร์เฟซบรรทัดคำสั่ง (CLI) พร้อมเข้าสู่ระบบดังแสดงในภาพ



ภาพที่ 4.13 ภาพแสดงหน้าต่างคอนโซล PuTTY

ขั้นตอนที่ 4 ป้อนชื่อผู้ใช้ ชื่อผู้ใช้เริ่มต้นคือ cisco แล้วกด Enter



ภาพที่ 4.14 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนชื่อผู้ใช้

ขั้นตอนที่ 5 ป้อนรหัสผ่าน รหัสผ่านเริ่มต้นคือ cisco แล้วกด Enter

```
User Name:cisco
Password:*****
```

ภาพที่ 4.15 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนรหัสผ่านสำเร็จ

หลังจากเมื่อทำการป้อนชื่อผู้ใช้ และป้อนรหัสผ่าน ถูกต้องจะแสดงชื่อสวิตช์ขึ้นมาดังภาพ 4.16

```
User Name:cisco
Password:*****

SWB3F10#
```

ภาพที่ 4.16 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนชื่อผู้ใช้และป้อนรหัสผ่านสำเร็จ

ถ้ามีการป้อนชื่อผู้ใช้และรหัสผ่านไม่ถูกต้อง ในครั้งแรก ระบบจะให้ป้อนชื่อผู้ใช้และรหัสผ่านอีก 2 ครั้ง ถ้ายังป้อนชื่อผู้ใช้และรหัสผ่านไม่ถูกต้อง จะมีข้อความแจ้งว่า authentication failed และทำการปิดการเชื่อมต่อกับสวิตช์ทันที

```
User Name:ciscos
Password:*****

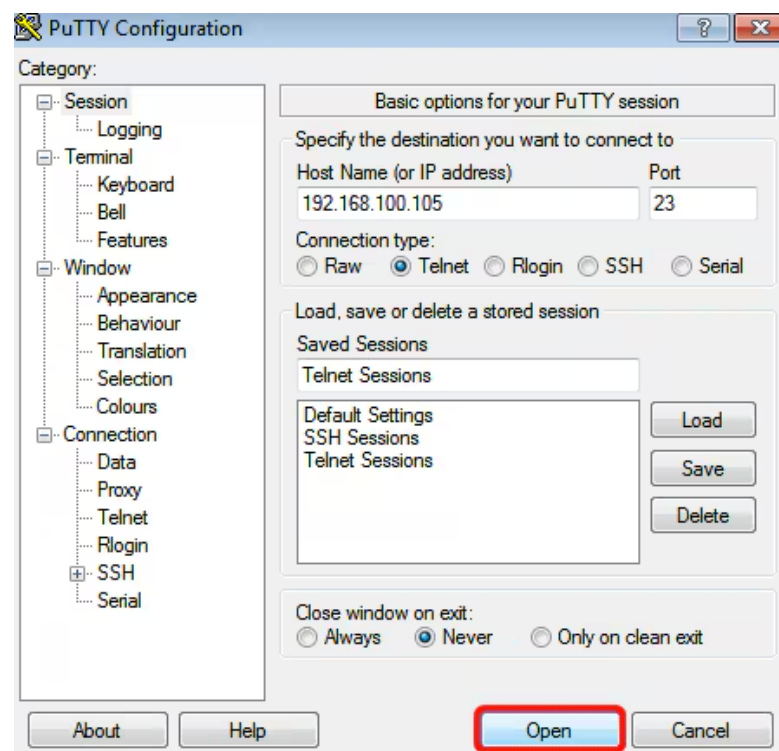
User Name:cisco
Password:*****

User Name:csicso
Password:*****
authentication failed
```

ภาพที่ 4.17 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนรหัสผ่านไม่สำเร็จ

Telnet เป็นการเข้าถึงอุปกรณ์จากระยะไกลที่ไม่มีการเข้ารหัส เพื่อไปบริหารจัดการ อุปกรณ์บนระบบเครือข่าย ซึ่งมักจะใช้ในอุปกรณ์ที่เก่าหรือในสภาพแวดล้อม เพื่อการทดสอบเท่านั้น ไม่แนะนำให้ใช้กับการใช้งานจริง

ขั้นตอนที่ 1. เปิดแอปพลิเคชัน PuTTY ไปที่ เมนู Session ป้อน Host name (or IP Address) แล้วเลือกเชื่อมต่อแบบ Telnet แล้วคลิก Open



ภาพที่ 4.18 ภาพแสดงหน้าต่าง Application PuTTY ที่เชื่อมต่อแบบ Telnet

จากนั้นหน้าต่างคอนโซล PuTTY จะเปิดขึ้น แล้วกด Enter บนแป้นพิมพ์ เพื่อเปิดใช้งานอินเทอร์เฟซบรรทัดคำสั่ง (CLI) พร้อมเข้าสู่ระบบดังแสดงในภาพ



ภาพที่ 4.19 ภาพแสดงหน้าต่างคอนโซล PuTTY อินเทอร์เฟซบรรทัดคำสั่ง (CLI)

ขั้นตอนที่ 2 ป้อนชื่อผู้ใช้ ชื่อผู้ใช้เริ่มต้นคือ cisco แล้วกด Enter

```
User Name:cisco█
```

ภาพที่ 4.20 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนชื่อผู้ใช้

ขั้นตอนที่ 3 ป้อนรหัสผ่าน รหัสผ่านเริ่มต้นคือ cisco แล้วกด Enter

```
User Name:cisco
Password:*****█
```

ภาพที่ 4.21 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนรหัสผ่านสำเร็จ

หลังจากเมื่อทำการป้อนชื่อผู้ใช้ และป้อนรหัสผ่าน ถูกต้องจะแสดงชื่อสวิตช์ขึ้นมาดังรูป

```
User Name:cisco
Password:*****

SWB3F10#█
```

ภาพที่ 4.22 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนรหัสผ่านสำเร็จ

ถ้ามีการป้อนชื่อผู้ใช้และรหัสผ่านไม่ถูกต้อง ในครั้งแรก ระบบจะให้ป้อนชื่อผู้ใช้และรหัสผ่านอีก 2 ครั้ง ถ้ายังป้อนชื่อผู้ใช้และรหัสผ่านไม่ถูกต้อง จะมีข้อความแจ้งว่า authentication failed และทำการปิดการเชื่อมต่อกับสวิตช์ทันที

```
User Name:ciscos
Password:*****

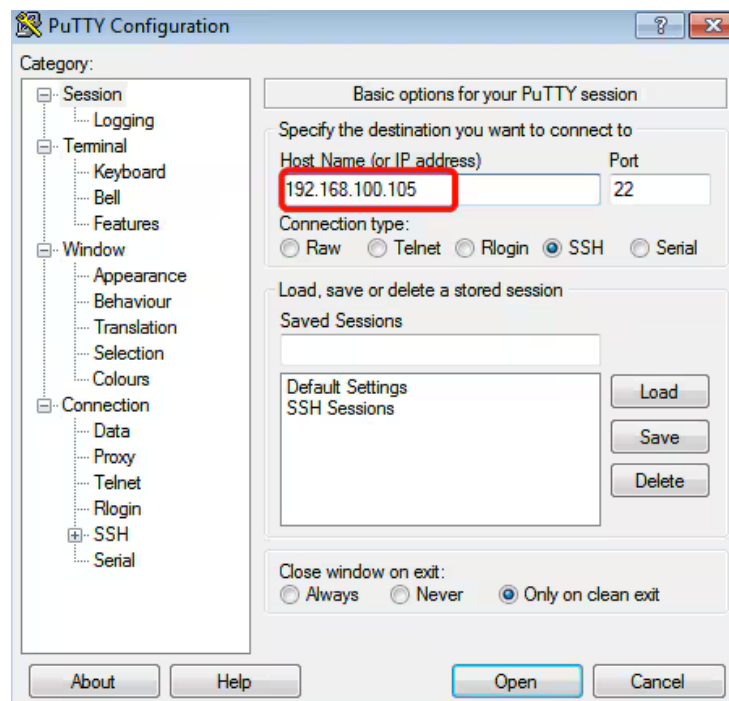
User Name:cisco
Password:*****

User Name:csicso
Password:*****
authentication failed
```

ภาพที่ 4.23 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนรหัสผ่านไม่สำเร็จ

Secure Shell (SSH) เป็นการเข้าถึงอุปกรณ์จากระยะไกล เพื่อเข้าไปยังอุปกรณ์ที่ ต้องการบริหารจัดการผ่านทางระบบเครือข่าย โดยที่ตัวอุปกรณ์เองต้องมีหมายเลข IP Address สำหรับ บริหารจัดการและเชื่อมต่อกับระบบเครือข่ายจึงจะใช้งาน SSH ได้ วิธีการนี้แนะนำ ให้ใช้เป็นหลัก หลังจากติดตั้งอุปกรณ์แล้ว เพื่อเข้าถึงอุปกรณ์เพราะมีความปลอดภัย เนื่องจากมีการเข้ารหัสข้อมูลที่ ส่งผ่าน SSH

ขั้นตอนที่ 1. เปิดแอปพลิเคชัน PuTTY ไปที่ เมนู Session ป้อน Host name (or IP Address) แล้วเลือกเชื่อมต่อแบบ SSH แล้วคลิก Open



ภาพที่ 4.24 ภาพแสดงหน้าต่าง Application PuTTY ที่เชื่อมต่อแบบ SSH

จากนั้นหน้าต่างคอนโซล PuTTY จะเปิดขึ้น แล้วกด Enter บนแป้นพิมพ์ เพื่อเปิดใช้งานอินเทอร์เฟซบรรทัดคำสั่ง (CLI) พร้อมเข้าสู่ระบบดังแสดงในภาพ



ภาพที่ 4.25 ภาพแสดงหน้าต่างคอนโซล PuTTY อินเทอร์เฟซบรรทัดคำสั่ง (CLI)

ขั้นตอนที่ 2 ป้อนชื่อผู้ใช้ ชื่อผู้ใช้เริ่มต้นคือ cisco แล้วกด Enter



ภาพที่ 4.26 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนชื่อผู้ใช้

ขั้นตอนที่ 3 ป้อนรหัสผ่าน รหัสผ่านเริ่มต้นคือ cisco แล้วกด Enter

```
User Name:cisco
Password:*****
```

ภาพที่ 4.27 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนรหัสผ่านสำเร็จ

หลังจากเมื่อทำการป้อนชื่อผู้ใช้ และป้อนรหัสผ่าน ถูกต้องจะแสดงชื่อสวิตช์ขึ้นมาดังรูป

```
User Name:cisco
Password:*****

SWB3F10#
```

ภาพที่ 4.28 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนรหัสผ่านสำเร็จ

ถ้ามีการป้อนชื่อผู้ใช้และรหัสผ่านไม่ถูกต้อง ในครั้งแรก ระบบจะให้ป้อนชื่อผู้ใช้และรหัสผ่านอีก 2 ครั้ง ถ้ายังป้อนชื่อผู้ใช้และรหัสผ่านไม่ถูกต้อง จะมีข้อความแจ้งว่า authentication failed และทำการปิดการเชื่อมต่อกับสวิตช์ทันที

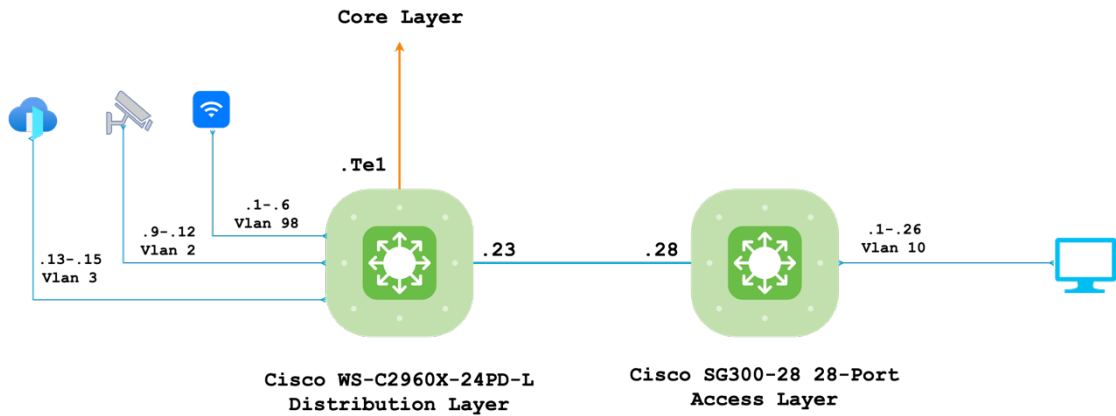
```
User Name:ciscos
Password:*****

User Name:cisco
Password:*****

User Name:csicso
Password:*****
authentication failed
```

ภาพที่ 4.29 ภาพแสดงหน้าต่างคอนโซล PuTTY ป้อนรหัสผ่านไม่สำเร็จ

ตัวอย่างรูปแบบการเชื่อมต่อ Switch Access Layer เข้ากับ Switch Distribution Layer



ภาพที่ 4.30 แผนผังการเชื่อมต่อ Switch Access Layer เข้ากับ Switch Distribution Layer

การเชื่อมต่ออุปกรณ์ที่นำไปติดตั้งในระดับ Distribution Layer นั้น สำหรับหน่วยงานจะใช้ อุปกรณ์สวิตช์ รุ่น Cisco WS-C2960X-24PD-L ดังภาพที่ 4.31



ภาพที่ 4.31 อุปกรณ์สวิตช์ Cisco WS-C2960X-24PD-L

โดยที่ตัวอุปกรณ์สวิตช์ รุ่น Cisco WS-C2960X-24PD-L มี 24 port มีความเร็ว 10/100/1000 Ethernet PoE+ ports สำหรับเชื่อมต่อ ด้วยสาย UTP และส่วนที่ใช้สายสัญญาณใยแก้วนำแสงนั้น จะมี 2 พอร์ต ความเร็ว 10G SFP+ การตั้งค่าพื้นฐานที่จำเป็นสำหรับอุปกรณ์ที่จะนำไปติดตั้งให้สามารถทำงานได้ตามที่ออกแบบไว้นั้น การตั้งค่าที่จำเป็นสำหรับ อุปกรณ์ Switch ดังต่อไปนี้

- **ตัวหนา** คือ คำสั่ง
 - **ตัวเอียง** คือ ตัวแปรที่ต้องใส่
1. ต้องเปิดใช้งานโหมด EXEC ที่มีสิทธิ์พิเศษ ป้อนรหัสผ่าน หากระบบถาม

คำสั่ง :

enable

ตัวอย่าง :

Switch > **enable**การเข้าสู่โหมดการกำหนดค่า

2. การเข้าสู่โหมดการกำหนดค่า

คำสั่ง :

```
configure terminal
```

ตัวอย่าง :

```
Switch # configure terminal
```

3. ทำการตั้งชื่อของอุปกรณ์มีการกำหนดดังนี้ ชื่อรุ่นสวิตช์ + อักษรย่อภาษาอังกฤษของตึกที่ทำ
ทำการติดตั้ง + ชั้นที่ทำการติดตั้ง + ห้องที่ทำการติดตั้ง + ลำดับสวิตช์ภายในตึก

คำสั่ง :

```
hostname [name]
```

ตัวอย่าง :

```
Switch (config)# hostname 2960AF2A20601
```

4. ทำการตั้งหมายเลข IP Address ของ gateway ให้อุปกรณ์ให้สามารถติดต่อกับ เครือข่าย
ภายนอกเพื่อการบริหารจัดการ ip default-gateway 192.168.99.1 ตามที่ได้ทำการ
จัดสรร IP Address เพื่อใช้งานภายในของสถาบันดนตรีกัลยาณีวัฒนา

คำสั่ง :

```
ip default-gateway [ ip address ]
```

ตัวอย่าง :

```
Switch (config)# ip default-gateway 192.168.99.1
```

5. ทำการเพิ่ม IP Address ของ NTP server เพื่อให้อุปกรณ์ตั้งเวลาให้ตรงกับ อุปกรณ์อื่น ๆ
ระบบเครือข่าย ไปที่ clock.nectec.or.th คือ IP Address: 202.44.204.114

คำสั่ง :

```
clock source sntp
```

```
sntp unicast client enable
```

```
sntp server [ ip address ] poll
```

```
clock timezone TH +7
```

ตัวอย่าง :

```
Switch (config)# clock source sntp
```

```
Switch (config)# sntp unicast client enable
```

```
Switch (config)# sntp server 202.44.204.114 poll
```

```
Switch (config)# clock timezone TH +7
```

6. เปิดการใช้งาน SNMP เพื่อให้อุปกรณ์ส่งค่าสำหรับการมอนิเตอร์

คำสั่ง :

```
snmp-server server
snmp-server community public ro view Default
snmp-server host [ ip address ] traps version [ 1,2,3 ]
```

ตัวอย่าง :

```
Switch (config)# snmp-server server
Switch (config)# snmp-server community public ro view Default
Switch (config)# snmp-server host 192.168.110.35 traps version 1
public
```

7. ทำการตั้งค่าที่อยู่ IP ของสวิตช์ ตามที่ได้ทำการออกแบบไว้

คำสั่ง :

```
interface vlan [ หมายเลข ]
ip address [ หมายเลข IP Address ] [ หมายเลข Subnet Mask ]
no ip address dhcp
```

ตัวอย่าง :

```
Switch (config)# interface vlan 99
Switch (config-vlan)# ip address 192.168.99.111 255.255.255.0
Switch (config-vlan)# no ip address dhcp
```

8. ทำการตั้งค่า interface ของสวิตช์ สำหรับเชื่อมต่อกับ Core Layer สวิตช์ (Interface up link)
ในที่นี้กำหนดให้ interface TenGigabitEthernet 1/0/1 เป็น Port สำหรับเชื่อมต่อ

คำสั่ง :

```
interface TenGigabitEthernet [ หมายเลข Port ]
description [ รายละเอียด ]
switchport mode trunk
```

ตัวอย่าง :

```
Switch (config)# interface TenGigabitEthernet 1/0/1
Switch (config-if)# description Uplink_to_Coreswitch
Switch (config-if)# switchport mode trunk
```

9. ทำการตั้งค่า interface ของสวิตช์ สำหรับเชื่อมต่อกับ Wireless Access Point ในที่นี้ กำหนดให้ interface GigabitEthernet1/0/1-6 เป็น Port สำหรับเชื่อมต่อ

คำสั่ง :

```
interface range gigabitethernet [ หมายเลขแรก - หมายเลขสุดท้าย ]
description [ รายละเอียด ]
switchport access vlan [ หมายเลข ]
switchport trunk native vlan [ หมายเลข ]
switchport trunk allowed vlan [ หมายเลข ]
switchport mode trunk
```

ตัวอย่าง :

```
Switch (config)# interface range gigabitethernet 1/0/1-6
Switch (config-if)# description Wireless_Access_Point
Switch (config-if)# switchport access vlan 98
Switch (config-if)# switchport trunk native vlan 98
Switch (config-if)# switchport trunk allowed vlan 6,9,98
Switch (config-if)# switchport mode trunk
```

10. ทำการตั้งค่า interface ของสวิตช์ สำหรับเชื่อมต่อกับกล้องวงจรปิดในที่นี้กำหนดให้ interface GigabitEthernet1/0/9-12 เป็น Port สำหรับเชื่อมต่อ

คำสั่ง :

```
interface range gigabitethernet [ หมายเลขแรก - หมายเลขสุดท้าย ]
description [ รายละเอียด ]
switchport mode access
switchport access vlan [ หมายเลข ]
```

ตัวอย่าง :

```
Switch (config)# interface range GigabitEthernet 1/0/9-12
Switch (config-if-range)# description IP_Camera
Switch (config-if-range)# switchport mode access
Switch (config-if-range)# switchport access vlan 2
```

11. ทำการตั้งค่า interface ของสวิตช์ สำหรับเชื่อมต่อกับระบบประตูอิเล็กทรอนิกส์ ในที่นี้ กำหนดให้ interface GigabitEthernet1/0/13-16 เป็น Port สำหรับเชื่อมต่อ

คำสั่ง :

```
interface range gigabitethernet [ หมายเลขแรก - หมายเลขสุดท้าย ]
description [ รายละเอียด ]
switchport mode access
switchport access vlan [ หมายเลข ]
```

ตัวอย่าง :

```
Switch (config)# interface range GigabitEthernet 1/0/13-15
Switch (config-if-range)# description Electronic_door
Switch (config-if-range)# switchport mode access
Switch (config-if-range)# switchport access vlan 3
```

เมื่อทำการตั้งค่าตามที่ได้กล่าวมาข้างต้นแล้วให้ทำการบันทึกค่า Config ของสวิตช์โดยให้ออกจากโหมดการกำหนดค่าแล้วจึงใช้คำสั่งบันทึกค่าลงบนหน่วยความจำของสวิตช์ และสวิตช์จะถามว่า Overwrite file [startup-config]... (Y/N)[N] ? ให้กดปุ่ม Y เพื่อต้องการให้ทำการบันทึก

คำสั่ง :

```
end
write memory
```

ตัวอย่าง :

```
Switch (config)# end
Switch # write memory
```

และการเชื่อมต่ออุปกรณ์ที่นำไปติดตั้งในระดับ Access Layer นั้น สำหรับหน่วยงานจะใช้ อุปกรณ์สวิตช์ รุ่น Cisco SG300-28 28-Port มีความเร็ว 10/100/1000 ดังภาพที่ 4.38



รูปด้านหน้า Cisco SG300-28



รูปด้านหลัง Cisco SG300-28

ภาพที่ 4.32 อุปกรณ์สวิตช์ Cisco SG300-28 28-Port 10/100/1000

โดยที่ตัวอุปกรณ์สวิตช์ รุ่น Cisco SG300-28 มี 26 port Gigabit Ethernet สำหรับเชื่อมต่อด้วยสาย UTP และส่วนที่ใช้สายสัญญาณใยแก้วนำแสงนั้น จะมี 2 แบบ คือ 2 พอร์ต Combo mini-GBIC (SFP) เลือกใช้งานได้ระหว่างพอร์ต RJ-45 และ SFP ความเร็ว 10/100/1000 Mbps สำหรับขยายการเชื่อมต่อ ดังนั้น การตั้งค่าพื้นฐานที่จำเป็นสำหรับอุปกรณ์ที่จะนำไปติดตั้งให้สามารถทำงานได้ตามที่ออกแบบไว้นั้น การตั้งค่าที่จำเป็นสำหรับ อุปกรณ์ Switch ดังต่อไปนี้

- **ตัวหนา** คือ คำสั่ง
- **ตัวเอียง** คือ ตัวแปรที่ต้องใส่

12. ต้องเปิดใช้งานโหมด EXEC ที่มีสิทธิพิเศษ ป้อนรหัสผ่าน หากระบบถาม

คำสั่ง :

enable

ตัวอย่าง :

Switch > **enable**

13. การเข้าสู่โหมดการกำหนดค่า

คำสั่ง :

configure terminal

ตัวอย่าง :

Switch # **configure terminal**

14. ทำการตั้งชื่อของอุปกรณ์มีการกำหนดดังนี้ ชื่อรุ่นสวิตช์ + อักษรย่อภาษาอังกฤษของตึกที่ทำ
ทำการติดตั้ง + ชั้นที่ทำการติดตั้ง + ห้องที่ทำการติดตั้ง + ลำดับสวิตช์ภายในตึก

คำสั่ง :

hostname [name]

ตัวอย่าง :

Switch (config)# **hostname SG300AF2A20603**

15. ทำการตั้งหมายเลข IP Address ของ gateway ให้อุปกรณ์ให้สามารถติดต่อกับ เครือข่ายภายนอกเพื่อการบริหารจัดการ ip default-gateway 192.168.99.1 ตามที่ได้ทำการจัดสรร IP Address

คำสั่ง :

```
ip default-gateway [ ip address ]
```

ตัวอย่าง :

```
Switch (config)# ip default-gateway 192.168.99.1
```

16. ทำการเพิ่ม IP Address ของ NTP server เพื่อให้อุปกรณ์ตั้งเวลาให้ตรงกับ อุปกรณ์อื่น ๆ ระบบเครือข่าย ไปที่ clock.nectec.or.th คือ IP Address: 202.44.204.114

คำสั่ง :

```
clock source sntp  
sntp unicast client enable  
sntp server [ ip address ] poll  
clock timezone TH +7
```

ตัวอย่าง :

```
Switch (config)# clock source sntp  
Switch (config)# sntp unicast client enable  
Switch (config)# sntp server 202.44.204.114 poll  
Switch (config)# clock timezone TH +7
```

17. เปิดการใช้งาน SNMP เพื่อให้อุปกรณ์ส่งค่าสำหรับการมอนิเตอร์

คำสั่ง :

```
snmp-server server  
snmp-server community public ro view Default  
snmp-server host [ ip address ] traps version [ 1,2,3 ]
```

ตัวอย่าง :

```
Switch (config)# snmp-server server  
Switch (config)# snmp-server community public ro view Default  
Switch (config)# snmp-server host 192.168.110.35 traps version 1
```

public

18. การเพิ่ม Vlan ให้กับอุปกรณ์สวิตช์ สำหรับการใช้งาน Vlan ตามที่ได้ทำการออกแบบไว้

คำสั่ง :

```
vlan database
vlan [ หมายเลข ]
```

ตัวอย่าง :

```
Switch (config)#vlan database
Switch (config-vlan)#vlan 99
Switch (config-vlan)#vlan 10
Switch (config-vlan)#vlan 3
```

19. ทำการตั้งค่าที่อยู่ IP ของสวิตช์ ตามที่ได้ทำการออกแบบไว้

คำสั่ง :

```
interface vlan [ หมายเลข ]
ip address [ หมายเลข IP Address ] [ หมายเลข Subnet Mask ]
no ip address dhcp
```

ตัวอย่าง :

```
Switch (config)# interface vlan 99
Switch (config-vlan)# ip address 192.168.99.113 255.255.255.0
Switch (config-vlan)# no ip address dhcp
```

20. ทำการตั้งค่า interface ของสวิตช์ สำหรับเชื่อมต่อกับ Distribution Layer สวิตช์ (Interface up link) ในที่นี้กำหนดให้ interface gigabitethernet28 เป็น Port สำหรับเชื่อมต่อ

คำสั่ง :

```
interface gigabitethernet [ หมายเลข Port]
description [ รายละเอียด ]
switchport trunk allowed vlan add [ หมายเลข vlan ตามที่ได้ลงทะเบียน]
```

ตัวอย่าง :

```
Switch (config)# interface gigabitethernet 28
Switch (config-if)# description Uplink_to_SW2960
Switch (config-if)# switchport trunk allowed vlan add 10,3,99
```

21. ทำการตั้งค่า Vlan ให้กับสวิตช์พอร์ตสำหรับเชื่อมต่อกับอุปกรณ์ต่าง ๆ ตามที่ได้ทำการ
ออกแบบไว้

กรณีที่เป็นคำสั่งกำหนดค่าสวิตช์พอร์ตเดียว

คำสั่ง :

```
interface gigabitethernet [ หมายเลข ]  
switchport mode access  
switchport access vlan [ หมายเลข ]
```

ตัวอย่าง :

```
Switch (config)# interface range GigabitEthernet 1  
Switch (config-if)# switchport mode access  
Switch (config-if)# switchport access vlan 10
```

กรณีที่เป็นคำสั่งกำหนดค่าช่วงของสวิตช์พอร์ต:

คำสั่ง :

```
interface range gigabitethernet [ หมายเลขแรก - หมายเลขสุดท้าย ]  
switchport mode access  
switchport access vlan [ หมายเลข ]
```

ตัวอย่าง :

```
Switch (config)# interface range GigabitEthernet 1-26  
Switch (config-if-range)# switchport mode access  
Switch (config-if-range)# switchport access vlan 10
```

เมื่อทำการตั้งค่าตามที่ได้กล่าวมาข้างต้นแล้วให้ทำการบันทึกค่า Config ของสวิตช์โดยให้ออกจาก
โหมดการกำหนดค่าแล้วจึงใช้คำสั่งบันทึกค่าลงบนหน่วยความจำของสวิตช์ และสวิตช์จะถามว่า
Overwrite file [startup-config].... (Y/N)[N] ? ให้กดปุ่ม Y เพื่อต้องการให้ทำการบันทึก

คำสั่ง :

```
end  
write memory
```

ตัวอย่าง :

```
Switch (config)# end  
Switch # write memory
```

การติดตั้งอุปกรณ์และเชื่อมต่อให้ใช้งาน

เตรียมเครื่องมือติดตั้งให้พร้อมตามชุดเครื่องมือเบื้องต้นสำหรับติดตั้งสำหรับอุปกรณ์สวิตช์ (Switch) ดังภาพที่ 4.6

ขั้นตอนการติดตั้งอุปกรณ์

1. เลือกตำแหน่งติดตั้งอุปกรณ์ภายในตู้แร็ค
2. ตรวจสอบปลั๊กรางภายในตู้แร็ค ว่าสามารถรองรับกระแสไฟเพียงพอหรือไม่
3. ระบุอุปกรณ์ระบบเครือข่ายปลายทางที่ต้องการเชื่อมต่อกับอุปกรณ์ใหม่
4. เลือกชนิดของสายสัญญาณที่ต้องการติดตั้ง
5. ตรวจสอบเส้นทางการเดินสัญญาณจากต้นทางจนถึงปลายทางว่าสามารถติดตั้งสายสัญญาณได้
6. หากไม่สามารถปฏิบัติตามข้อ 1- 5 ได้ ให้กลับไปทำข้อ 1 ใหม่
7. เมื่อตรวจทุกอย่างเรียบร้อยแล้วให้ดำเนินการติดตั้งอุปกรณ์เข้าไปในตู้แร็คได้
8. เปิดใช้งานอุปกรณ์ที่ติดตั้งใหม่
9. เชื่อมต่อสายสัญญาณให้ตรงกับที่ตั้งแค้
10. รอจนอุปกรณ์เริ่มทำงาน

ขั้นตอนที่ 5 ทดสอบการใช้งาน

1. ทำการใช้คำสั่งสำหรับตรวจสอบการเชื่อมต่อเครือข่าย โดยใช้คำสั่ง Ping ไปที่

```
ip gateway 192.168.99.1
```

```
2960AF2A20401#ping 10.200.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.200.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
2960AF2A20401#
```

ภาพที่ 4.33 การใช้คำสั่ง Ping ไปที่ ip gateway 192.168.99.1

2. ใช้คำสั่ง Ping จาก 192.168.99.111 (hostname 2960AF2A20601) ไปที่ IP Address 192.168.99.113 (hostname SG300AF2A20603)

```
2960AF2A20401#ping 10.200.99.113
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.200.99.113, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/8/14 ms
2960AF2A20401#
```

ภาพที่ 4.34 การใช้คำสั่ง Ping จาก 192.168.99.111 ไปที่ IP Address 192.168.99.113

- ใช้คำสั่ง show interfaces status เพื่อทำการตรวจสอบว่า Cisco WS-C2960X-24PD-L ได้ทำการตั้งค่า ตามที่ได้ออกแบบไว้หรือไม่ และสถานะเป็นอย่างไร

```

2960AF2A20401#sh interfaces status
Port      Name                Status      Vlan    Duplex  Speed  Type
-----
Gi1/0/1   "AP-A209"           connected   trunk   a-full  a-1000 10/100/1000BaseTX
Gi1/0/2   Connect to Access   connected   trunk   a-full  a-1000 10/100/1000BaseTX
Gi1/0/3   WIFI A3_Office_1    connected   trunk   a-full  a-1000 10/100/1000BaseTX
Gi1/0/4   WIFI A_Office_Zone  connected   trunk   a-full  a-1000 10/100/1000BaseTX
Gi1/0/5   AP-VIPROOM          connected   trunk   a-full  a-1000 10/100/1000BaseTX
Gi1/0/6   AP-A207             connected   trunk   a-full  a-1000 10/100/1000BaseTX
Gi1/0/7   To A209 Port C16    notconnect  111     auto    auto    10/100/1000BaseTX
Gi1/0/8   disabled            disabled    10      auto    auto    10/100/1000BaseTX
Gi1/0/9   Network To Switch   connected   2       a-full  a-1000 10/100/1000BaseTX
Gi1/0/10  IP Camera A209      connected   2       a-full  a-100  10/100/1000BaseTX
Gi1/0/11  IP Camera A209      connected   2       a-full  a-100  10/100/1000BaseTX
Gi1/0/12  IP Camera A209      connected   2       a-full  a-100  10/100/1000BaseTX
Gi1/0/13  notconnect          notconnect  3       auto    auto    10/100/1000BaseTX
Gi1/0/14  notconnect          notconnect  3       auto    auto    10/100/1000BaseTX
Gi1/0/15  notconnect          notconnect  3       auto    auto    10/100/1000BaseTX
Gi1/0/16  connected            connected   4       a-full  a-1000 10/100/1000BaseTX
Gi1/0/17  APWIFI-A210         connected   trunk   a-full  a-1000 10/100/1000BaseTX
Gi1/0/18  notconnect          notconnect  1       auto    auto    10/100/1000BaseTX
Gi1/0/19  connected            connected   6       a-full  a-100  10/100/1000BaseTX
Gi1/0/20  notconnect          notconnect  10      auto    auto    10/100/1000BaseTX
Gi1/0/21  notconnect          notconnect  4       auto    auto    10/100/1000BaseTX
Gi1/0/22  connected            connected   10      a-full  a-1000 10/100/1000BaseTX
Gi1/0/23  to SG300            connected   trunk   a-full  a-1000 10/100/1000BaseTX
Gi1/0/24  notconnect          notconnect  10      auto    auto    10/100/1000BaseTX
Te1/0/1   UpLink to Core      connected   trunk   full    10G    SFP-10GBaseLR
Te1/0/2   notconnect          notconnect  1       full    10G    Not Present
Fa0/24   notconnect          notconnect  routed  auto    auto    10/100BaseTX

```

ภาพที่ 4.35 ใช้คำสั่ง show interfaces status เพื่อทำการตรวจสอบการตั้งค่าของ Cisco WS-C2960X-24PD-L

- ใช้คำสั่ง Show Vlan เพื่อทำการตรวจสอบว่า Cisco SG300-28 ได้ทำการตั้งค่าถูกต้อง ตามที่ได้ออกแบบไว้หรือไม่ และสถานะเป็นอย่างไร

```

SG300AF2A20403#show vlan
Vlan      Name                Ports                Type      Authorization
-----
1         1                   Po1,Po3-8           Default   Required
2         2                   Po1-2               static    Required
3         3                   Po1-2               static    Required
4         4                   Po1-2               static    Required
6         6                   Po2                 static    Required
9         9                   static              static    Required
10        10                  g11-26,Po1-2        static    Required
11        11                  static              static    Required
12        12                  static              static    Required
13        13                  static              static    Required
14        14                  static              static    Required
15        15                  static              static    Required
20        20                  Po1-2               static    Required
30        30                  Po1-2               static    Required
40        40                  Po1-2               static    Required
50        50                  static              static    Required
60        60                  Po1-2               static    Required
97        97                  static              static    Required
98        98                  Po1-2               static    Required
99        99                  Po1-2               static    Required
100       100                 Po1-2               static    Required
110       110                 Po2                 static    Required
111       111                 Po1-2               static    Required
200       200                 Po1-2               static    Required

```

ภาพที่ 4.36 ใช้คำสั่ง show vlan เพื่อทำการตรวจสอบการตั้งค่าของ Cisco SG300-28

ขั้นตอนที่ 6 เพิ่มเข้าสู่ระบบ Monitoring

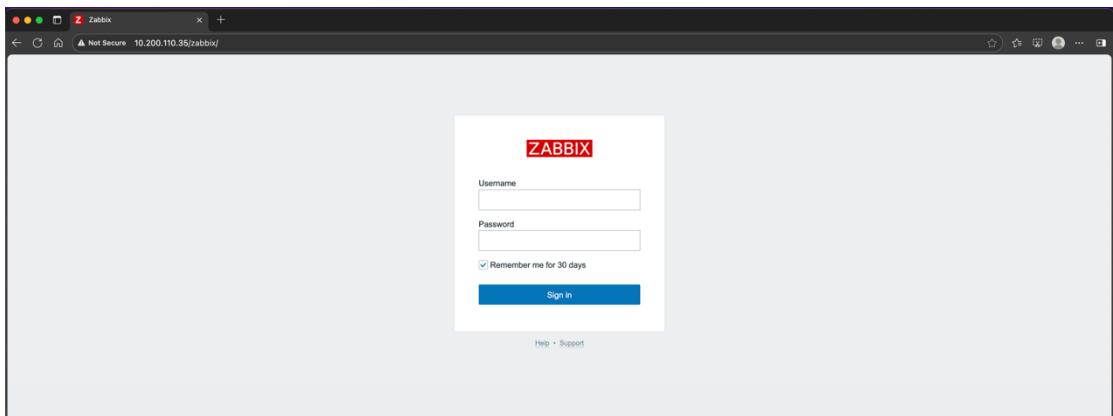
โดยสถาบันใช้ ZABBIX ระบบ Monitoring แบบ Open Source ที่ใช้สำหรับติดตามสถานะของระบบเครือข่าย เซิร์ฟเวอร์ แอปพลิเคชัน หรือบริการ IT ต่างๆ แบบเรียลไทม์ โดยมีขั้นตอนการเพิ่มอุปกรณ์ ดังนี้

1. ทำการเปิดเว็บเบราว์เซอร์ (web browser) เช่น Google Chrome, Firefox, และ microsoft edge แล้ว ป้อนที่อยู่ ระบบ Monitoring ดังนี้ <http://192.168.110.35/zabbix>



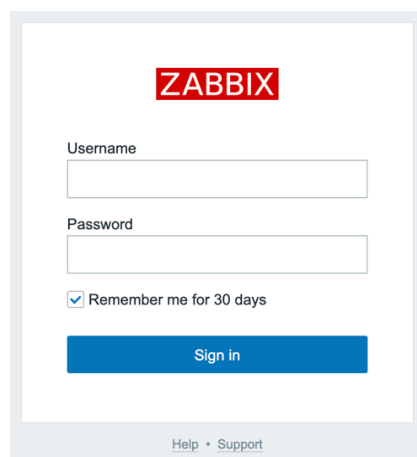
ภาพที่ 4.37 ป้อนที่อยู่เพื่อเข้าสู่ระบบ Monitoring

2. จากนั้นปรากฏหน้าต่างระบบ Monitoring (ZABBIX) พร้อมเข้าสู่ระบบดังแสดงในภาพที่ 4.38



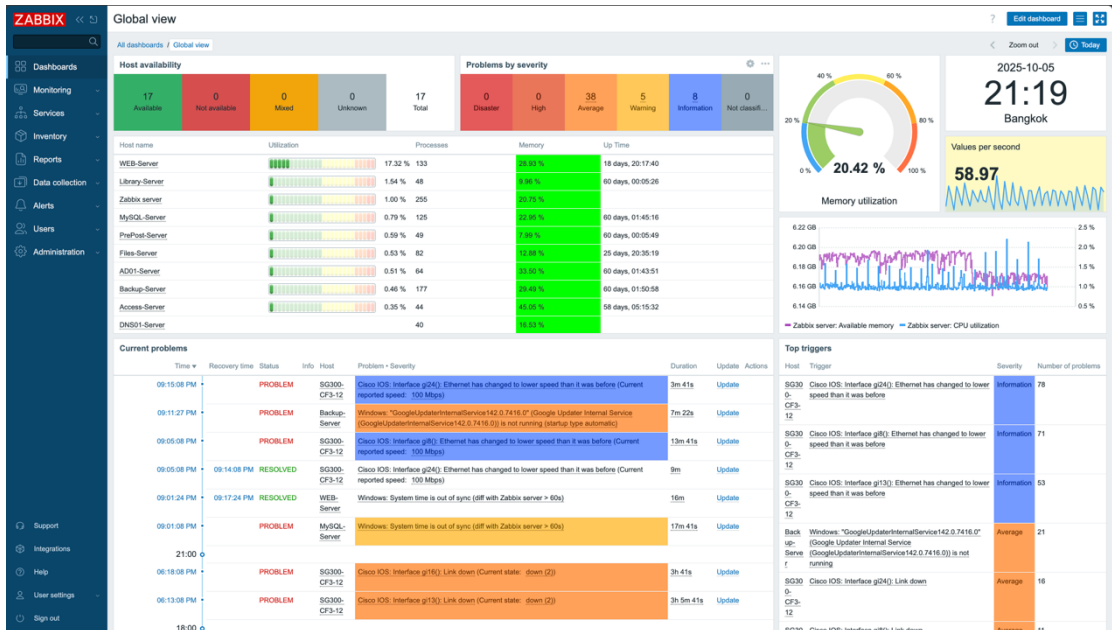
ภาพที่ 4.38 หน้าต่างระบบ Monitoring (ZABBIX) พร้อมเข้าสู่ระบบ

3. ให้ทำการป้อนชื่อผู้ใช้ และ ป้อนรหัสผ่าน ตามที่ได้ ได้สร้างขึ้นตั้งแต่ตอนติดตั้งระบบ แล้วกด Enter



ภาพที่ 4.39 หน้าต่างระบบ Monitoring (ZABBIX) การป้อนชื่อผู้ใช้และรหัสผ่าน

หลังจากเมื่อทำการป้อนชื่อผู้ใช้งาน และรหัสผ่าน ถูกต้องจะแสดงหน้าระบบ Monitoring (ZABBIX) ขึ้นมาดังรูป



ภาพที่ 4.40 หน้าต่างระบบ Monitoring (ZABBIX) หลังจากการเข้าสู่ระบบสำเร็จ

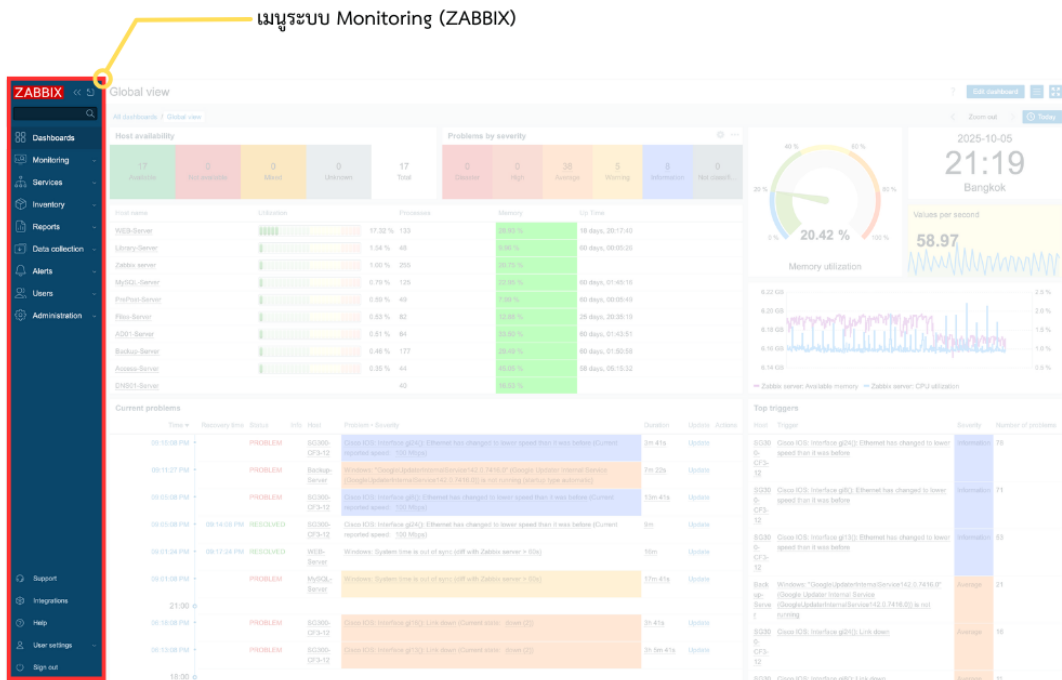
ถ้าป้อนชื่อผู้ใช้งาน / รหัสผ่านไม่ถูกต้อง บัญชีถูกล็อกชั่วคราวเนื่องจากความพยายามในการเข้าสู่ระบบ ให้ทำการติดต่อ ผู้ดูแลระบบ Monitoring (ZABBIX) ทำการปลดบล็อกผู้ใช้งานหรือรีเซ็ตรหัสผ่านใหม่

The screenshot shows the ZABBIX login page. At the top, the ZABBIX logo is displayed. Below it, there are input fields for 'Username' and 'Password'. A red error message is shown: 'Incorrect user name or password or account is temporarily blocked.' There is a checkbox for 'Remember me for 30 days' which is checked. A blue 'Sign in' button is at the bottom. At the very bottom, there are links for 'Help' and 'Support'.

ภาพที่ 4.41 หน้าต่างการแจ้งเตือนหลังจากการเข้าสู่ระบบไม่สำเร็จ

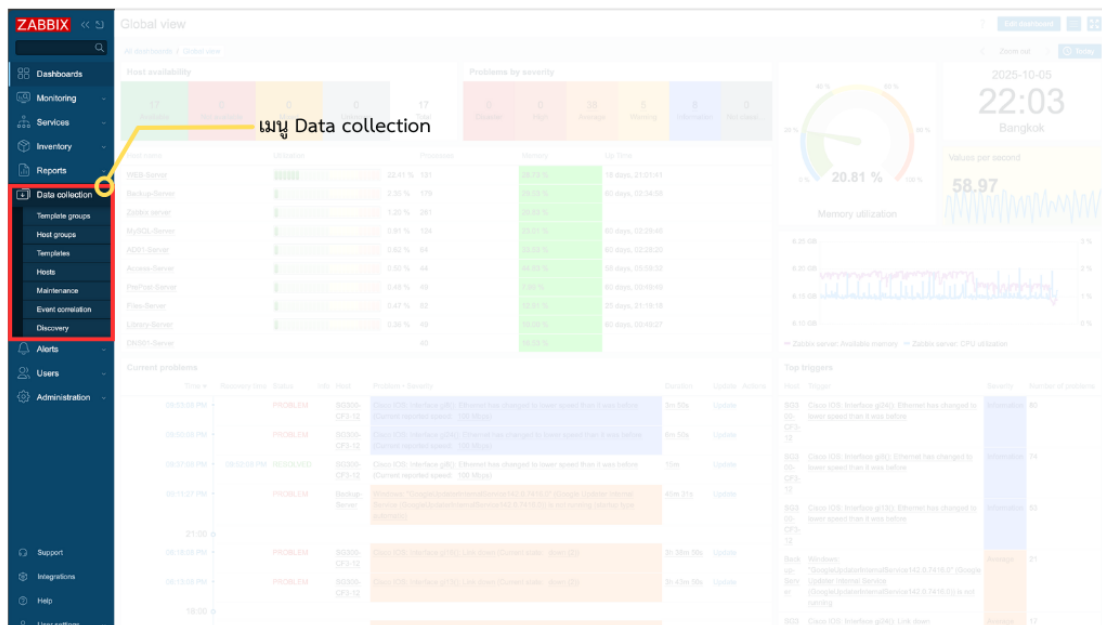
4. การเพิ่มอุปกรณ์สวิตช์ ระบบ Monitoring (ZABBIX) โดยให้ไปที่เมนูด้าน

ซ้ายมือดังภาพที่



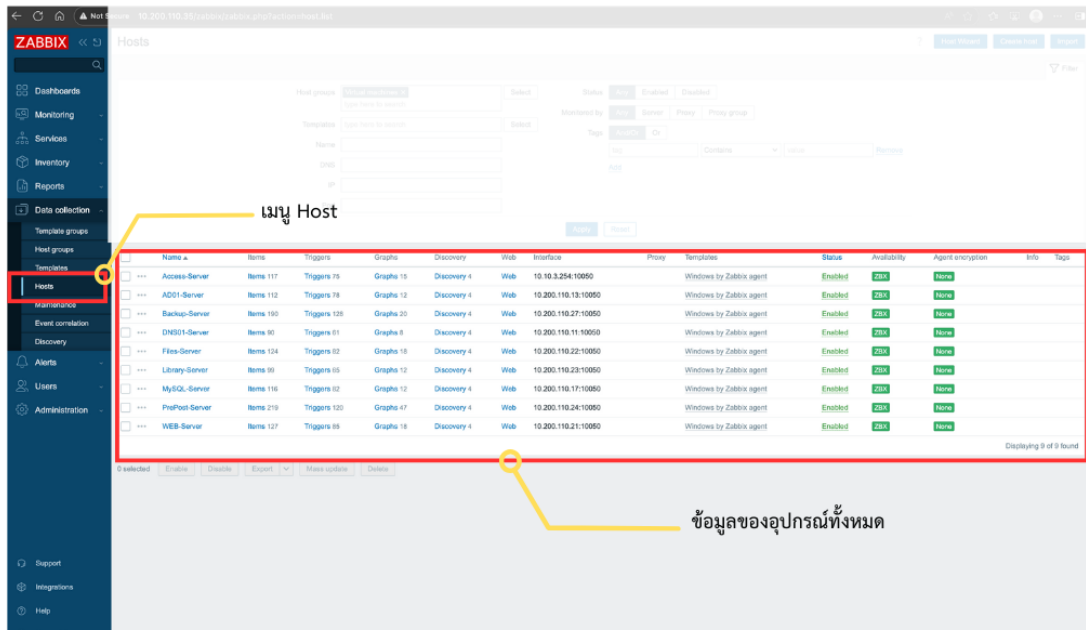
ภาพที่ 4.42 การแสดงเมนูบนระบบ Monitoring (ZABBIX)

5. ต่อมาให้หน้าเมาส์ ไปที่ เมนู Data collection แล้วทำการคลิก



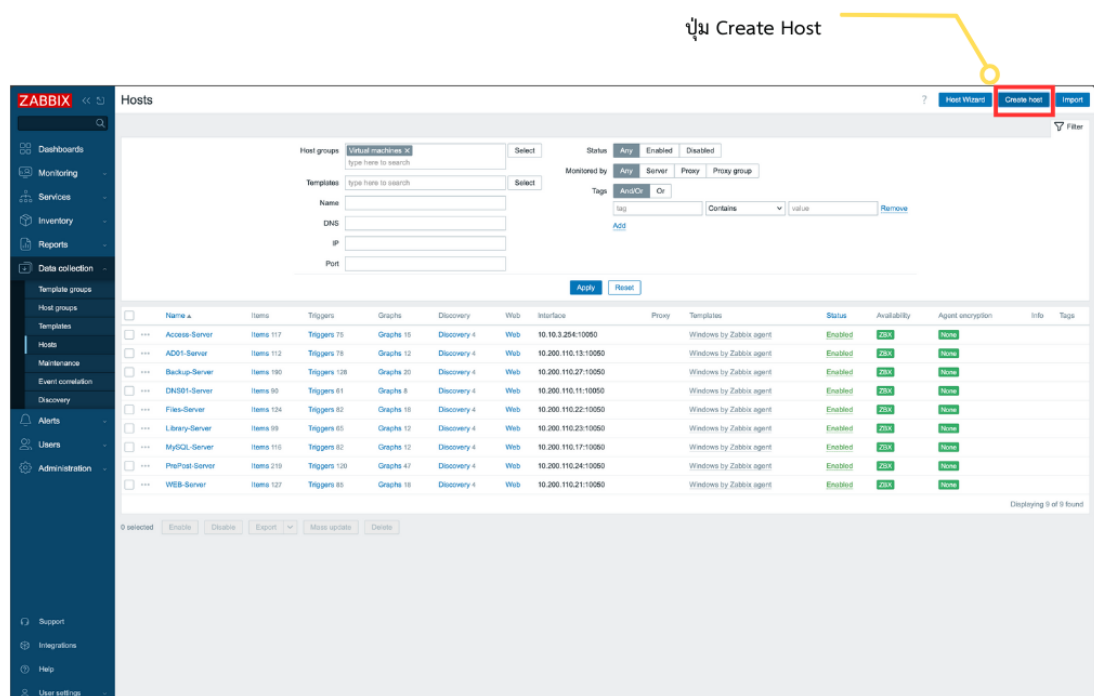
ภาพที่ 4.43 การแสดงเมนูบนระบบ Monitoring (ZABBIX) ในส่วน Data collection

6. ต่อมาให้หน้าเมาส์ ไปที่เมนูย่อย Host ของ เมนู Data collection จากนั้นให้ทำการคลิกที่เมนูย่อย Host เพื่อที่จะแสดงข้อมูลของอุปกรณ์ทั้งหมดที่มีในระบบ



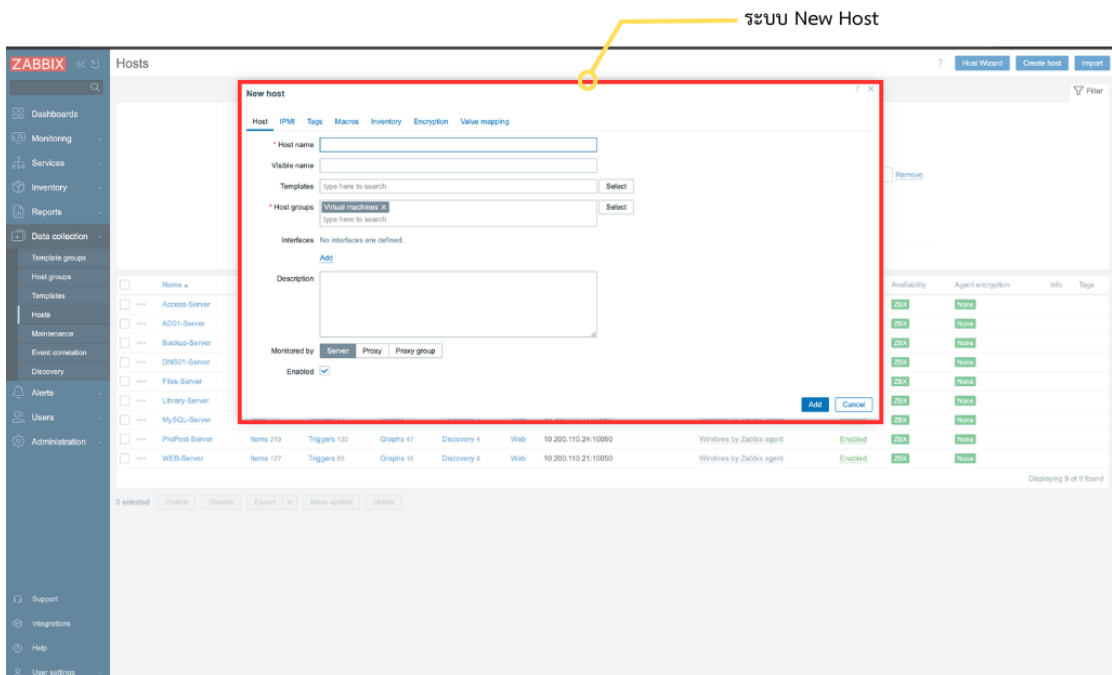
ภาพที่ 4.44 การแสดงเมนูระบบ Monitoring (ZABBIX) เมนูย่อย Host ของเมนู Data collection

7. เมื่อแสดงข้อมูลของอุปกรณ์ทั้งหมดที่มีในระบบให้หน้าเมาส์ ไปปุ่ม Create Host ที่ด้านขวาบน ดังภาพที่ 4.45 และให้ใช้เมาส์คลิกที่ปุ่ม



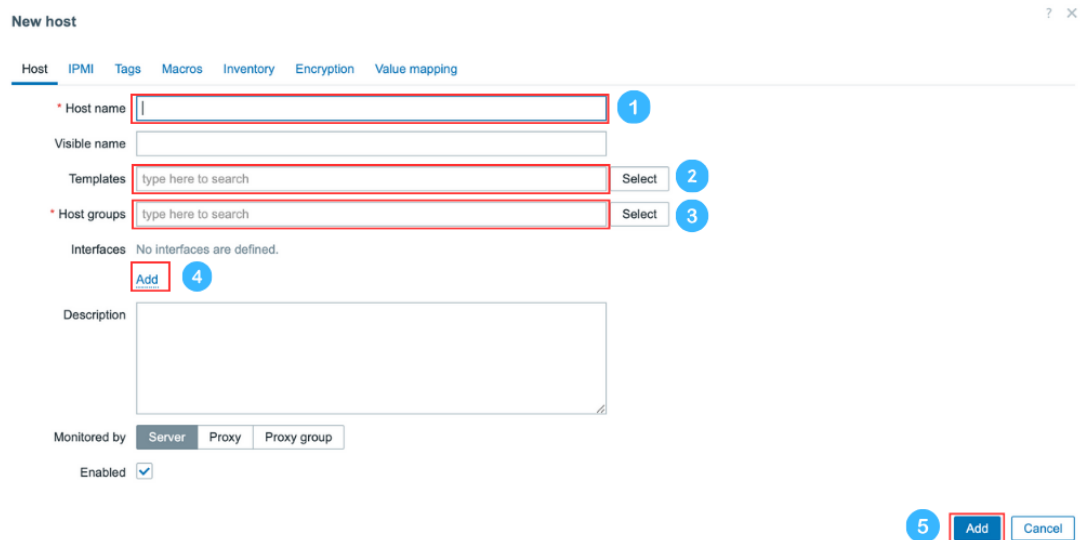
ภาพที่ 4.45 การแสดงเมนูระบบ Monitoring (ZABBIX) ปุ่ม Create Host

หลังจากทำการคลิกที่ปุ่ม Create Host แล้ว จะมีหน้าต่างระบบที่ชื่อว่า New Host ขึ้นมาดังรูปที่....



ภาพที่ 4.46 หน้าระบบที่ชื่อว่า New Host

8. การป้อนข้อมูลอุปกรณ์สวิตช์ ที่ได้ทำการติดตั้งเสร็จแล้ว ตัวอย่างเช่น อุปกรณ์สวิตช์ รุ่น Cisco WS-C2960X-24PD-L โดยมีทั้งหมด 5 ชั้นตอนดังนี้



ภาพที่ 4.47 หน้าระบบการป้อนข้อมูลอุปกรณ์สวิตช์

1. การตั้ง Host name ให้ทำการป้อนข้อมูลตามที่ได้ตั้งชื่ออุปกรณ์สวิตช์ไว้แล้ว เพื่อจะได้ทราบถึงว่าอุปกรณ์สวิตช์ชื่อรุ่นอะไร และทำการติดตั้งอยู่ที่ไหน เช่น 2960-AF2-A20601

New host

Host IPMI Tags Macros Inventory Encryption Value mapping

* Host name 2960-AF2-A20601

Visible name 2960-AF2-A20601

Templates type here to search Select

* Host groups type here to search Select

Interfaces No interfaces are defined.
Add

Description

Monitored by Server Proxy Proxy group

Enabled

Add Cancel

ภาพที่ 4.48 หน้าระบบการป้อนชื่ออุปกรณ์สวิตช์

2. การเพิ่ม Templates ให้ทำกดที่ปุ่ม Select

New host

Host IPMI Tags Macros Inventory Encryption Value mapping

* Host name 2960-AF2-A20601

Visible name 2960-AF2-A20601

Templates type here to search Select

* Host groups type here to search Select

Interfaces No interfaces are defined.
Add

Description

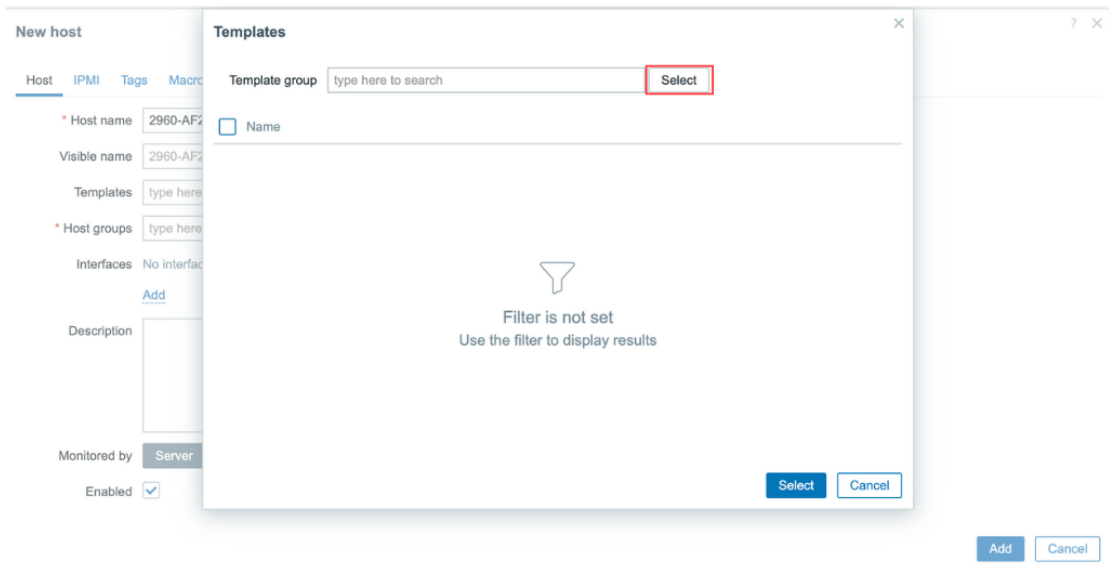
Monitored by Server Proxy Proxy group

Enabled

Add Cancel

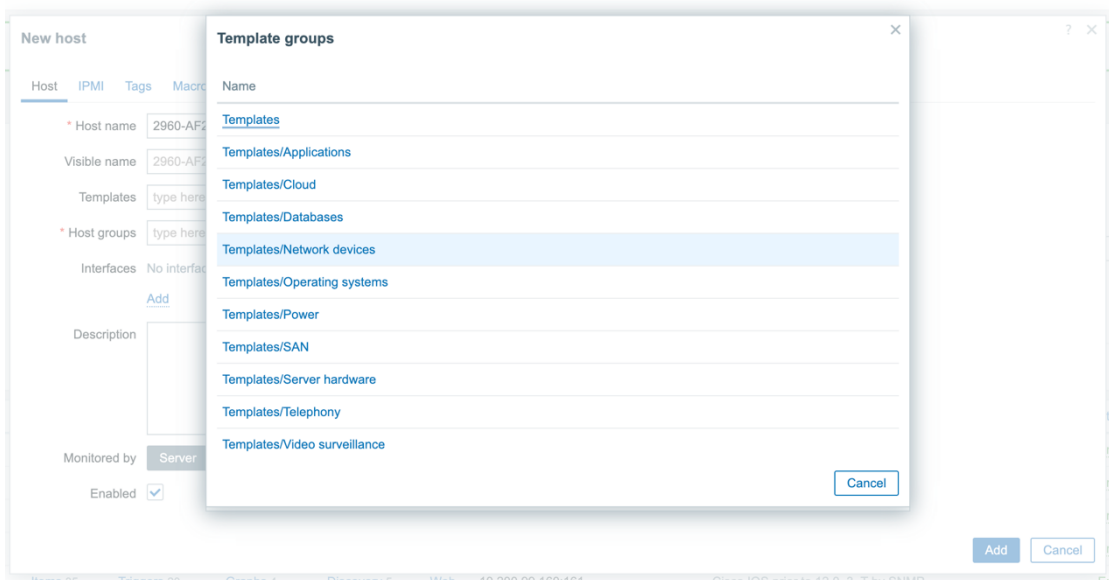
ภาพที่ 4.49 หน้าระบบการเพิ่ม Templates

ระบบจะแสดงหน้ารายการ Templates ขึ้นมา



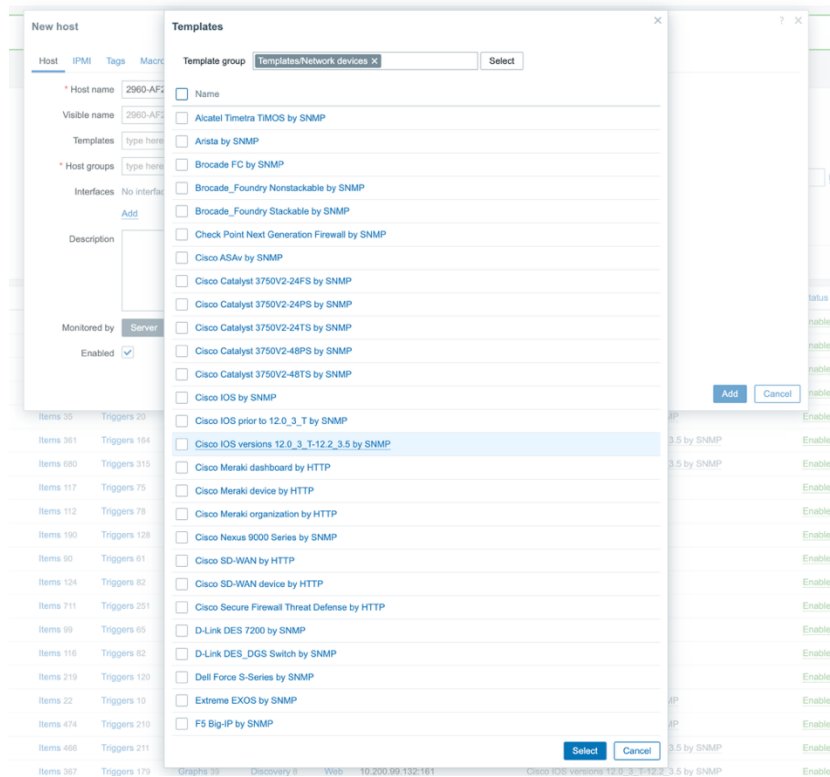
ภาพที่ 4.50 หน้าระบบรายการ Templates

ให้ทำคดที่ปุ่ม Select เพื่อทำการเลือก Template group ที่มีในระบบในที่นี่ อุปกรณ์ที่เราทำการติดตั้งนั้น เป็นอุปกรณ์ ประเภท Network ให้ทำการคลิกที่ Templates/Network devices ดังภาพ



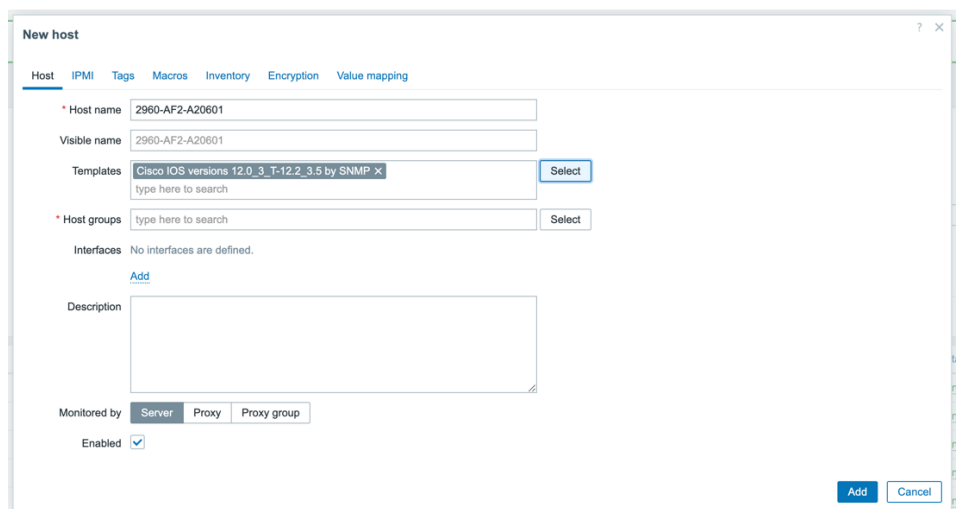
ภาพที่ 4.51 หน้าระบบรายการเลือก Templates

หลังจากทำการคลิกที่ Templates/Network devices ก็ จะแสดงรายการ Templates ของ Network devices ทั้งหมดที่มีในระบบ แล้วให้ทำการเลือกที่เป็น Cisco IOS versions 12.0_3_T-12.2_3.5 by SNMP เนื่องจาก อุปกรณ์ที่ทำการติดตั้งเป็นของยี่ห้อ Cisco เพื่อที่จะได้แสดงข้อมูลได้อย่างถูกต้อง และกดปุ่ม Select



ภาพที่ 4.52 หน้ารายการ Templates ของ Network devices

หลังจากทำการกรอกปุ่ม Select แล้วระบบจะเพิ่มข้อมูล Templates ที่เราต้องการดังภาพ



ภาพที่ 4.53 หน้าเพิ่มข้อมูล Templates

3. การเพิ่ม Host groups ให้ทำคดที่ปุ่ม Select

The screenshot shows the 'New host' configuration page. The 'Host groups' field is highlighted with a red box and a blue circle with the number '3'. The form includes the following fields and options:

- Host name: 2960-AF2-A20601
- Visible name: 2960-AF2-A20601
- Templates: Cisco IOS versions 12.0_3_T-12.2_3.5 by SNMP x (with a 'Select' button)
- Host groups: type here to search (with a 'Select' button)
- Interfaces: No interfaces are defined. (with an 'Add' button)
- Description: (empty text area)
- Monitored by: Server, Proxy, Proxy group
- Enabled:

Buttons: Add, Cancel

ภาพที่ 4.54 หน้าการเพิ่ม Host groups

ระบบจะแสดงหน้ารายการ Host groups ขึ้นมาตามที่เราได้จัดทำไว้แล้ว เมื่อระบบได้หน้า Host groups ขึ้นมาแล้ว ให้ทำการเลือกที่ Switch Network เนื่องจากอุปกรณ์ที่ทำการเพิ่มเข้าไปในระบบเป็นอุปกรณ์ ประเภท Switch Network ที่ต้องการการเลือกเสร็จแล้วให้กดปุ่ม Select

The screenshot shows the 'New host' configuration page with a 'Host groups' modal window open. The modal window displays a list of host groups with 'Switch Network' selected. The modal window has 'Select' and 'Cancel' buttons.

Host groups list:

- Applications
- Databases
- Discovered hosts
- Hypervisors
- Linux servers
- Switch Network
- Virtual machines
- Zabbix servers

Buttons: Select, Cancel

ภาพที่ 4.55 หน้ารายการ Host groups

หลังจากทำการการกดปุ่ม Select แล้วระบบจะเพิ่มข้อมูล Host groups ที่เราต้องการดังภาพ

New host

Host IPMI Tags Macros Inventory Encryption Value mapping

* Host name 2960-AF2-A20601

Visible name 2960-AF2-A20601

Templates Cisco IOS versions 12.0_3_T-12.2_3.5 by SNMP x Select
type here to search

* Host groups Switch Network x Select
type here to search

Interfaces No interfaces are defined.
Add

Description

Monitored by Server Proxy Proxy group

Enabled

Add Cancel

ภาพที่ 4.56 เพิ่มข้อมูล Host groups

4. การตั้งค่า Interfaces ให้ทำกดที่ปุ่ม Add

New host

Host IPMI Tags Macros Inventory Encryption Value mapping

* Host name 2960-AF2-A20601

Visible name 2960-AF2-A20601

Templates Cisco IOS versions 12.0_3_T-12.2_3.5 by SNMP x Select
type here to search

* Host groups Switch Network x Select
type here to search

Interfaces No interfaces are defined.
Add 4

Description

Monitored by Server Proxy Proxy group

Enabled

Add Cancel

ภาพที่ 4.57 การตั้งค่า Interfaces

หลังจากกดปุ่ม Add ระบบจะแสดงหน้ารายการประเภท Interfaces ที่จะส่งข้อมูลให้กลับระบบ Monitoring (ZABBIX) และจากการตั้งค่าของอุปกรณ์ สวิตช์ รุ่น Cisco WS-C2960X-24PD-L แล้ว และได้ทำการตั้งค่าการส่งข้อมูลเป็นแบบ SNMP V1 จึงให้ทำการคลิกที่เป็น SNMP

ภาพที่ 4.58 การตั้งค่าประเภทการส่งข้อมูล

หลังจากทำการคลิกแล้ว ก็จะแสดงการป้อนข้อมูลดังภาพที่....

ภาพที่ 4.59 การแสดงช่องสำหรับป้อนข้อมูลการส่งข้อมูล

หลังจากนั้น ให้ทำการป้อนข้อมูลของอุปกรณ์ สวิตช์ รุ่น Cisco WS-C2960X-24PD-L ตามที่ได้ตั้งค่าไว้แล้วในขั้นตอนการตั้งค่าที่ 6 และ ข้อมูลที่ 1 คือ หมายเลข IP Address ประจำเครื่องของ Cisco WS-C2960X-24PD-L

6. เปิดการใช้งาน SNMP เพื่อให้อุปกรณ์ส่งค่าสำหรับการมอนิเตอร์

คำสั่ง :

```
snmp-server server
```

```
snmp-server community public ro view Default
```

```
snmp-server host [ ip address ] traps version [ 1,2,3 ]
```

ตัวอย่าง :

```
Switch (config)# snmp-server server
```

```
Switch (config)# snmp-server community public ro view Default
```

```
Switch (config)# snmp-server host 10.200.110.35 traps version 1 public
```

ภาพที่ 4.60 การแสดงระบบ Monitoring (ZABBIX) การตั้งค่าป้อนข้อมูลการส่งข้อมูล

5. หลังจากป้อนข้อมูลครบหมดแล้วให้ทำการกดปุ่ม Add ระบบ Monitoring (ZABBIX) จะทำการบันทึกค่าและนำไปแสดง ข้อมูลในหน้าแสดงข้อมูลของอุปกรณ์ทั้งหมดที่มีในระบบ

Name	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption	Info	Tags
2500-WL-C252	Items 24	Triggers 0	Graphs 1	Discovery 6	Web	10.200.97.252-161		Cisco ICS by SNMP	Enabled	SNMP	None		
2500-WL-C253	Items 23	Triggers 0	Graphs 1	Discovery 6	Web	10.200.97.253-161		Cisco ICS by SNMP	Enabled	SNMP	None		
2800-AF-1-CON	Items 370	Triggers 168	Graphs 41	Discovery 7	Web	10.200.99.112-161		Cisco ICS versions 12.0_3_T-12.2_3.5 by SNMP	Enabled	SNMP	None		
2800-AF2-A20601	Items 343	Triggers 166	Graphs 39	Discovery 7	Web	10.200.99.111-161		Cisco ICS versions 12.0_3_T-12.2_3.5 by SNMP	Enabled	SNMP	None		
2800-WF-4-11	Items 35	Triggers 20	Graphs 4	Discovery 5	Web	10.200.99.180-161		Cisco ICS prior to 12.0_3_T by SNMP	Enabled	SNMP	None		
2800-POE-CF35	Items 381	Triggers 184	Graphs 40	Discovery 7	Web	10.200.100.17-161		Cisco ICS versions 12.0_3_T-12.2_3.5 by SNMP	Enabled	SNMP	None		
3600-CF2-IT	Items 350	Triggers 315	Graphs 74	Discovery 7	Web	10.200.95.142-161		Cisco ICS versions 12.0_3_T-12.2_3.5 by SNMP	Enabled	SNMP	None		
Access-Server	Items 117	Triggers 75	Graphs 15	Discovery 4	Web	10.10.3.254-10050		Windows by Zabbix agent	Enabled	ZBX	None		
AD01-Server	Items 112	Triggers 76	Graphs 12	Discovery 4	Web	10.200.110.13-10050		Windows by Zabbix agent	Enabled	ZBX	None		
Backup-Server	Items 190	Triggers 128	Graphs 20	Discovery 4	Web	10.200.110.27-10050		Windows by Zabbix agent	Enabled	ZBX	None		
DNS01-Server	Items 90	Triggers 61	Graphs 6	Discovery 4	Web	10.200.110.11-10050		Windows by Zabbix agent	Enabled	ZBX	None		
File-Server	Items 124	Triggers 62	Graphs 18	Discovery 4	Web	10.200.110.22-10050		Windows by Zabbix agent	Enabled	ZBX	None		
FortGate-200G	Items 711	Triggers 251	Graphs 102	Discovery 5	Web	10.200.100.250-161		FortGate by SNMP	Enabled	SNMP	None		
Library-Server	Items 99	Triggers 65	Graphs 12	Discovery 4	Web	10.200.110.23-10050		Windows by Zabbix agent	Enabled	ZBX	None		
MySQL-Server	Items 116	Triggers 62	Graphs 12	Discovery 4	Web	10.200.110.17-10050		Windows by Zabbix agent	Enabled	ZBX	None		
PrePost-Server	Items 219	Triggers 120	Graphs 47	Discovery 4	Web	10.200.110.24-10050		Windows by Zabbix agent	Enabled	ZBX	None		
SG300-AF2-22	Items 22	Triggers 10	Graphs 1	Discovery 5	Web	10.200.99.113-161		Cisco ICS prior to 12.0_3_T by SNMP	Enabled	SNMP	None		
SG300-CF-12	Items 474	Triggers 210	Graphs 50	Discovery 7	Web	10.200.99.130-161		Cisco ICS prior to 12.0_3_T by SNMP	Enabled	SNMP	None		
SG300-CF1-22	Items 466	Triggers 211	Graphs 48	Discovery 5	Web	10.200.99.131-161		Cisco ICS versions 12.0_3_T-12.2_3.5 by SNMP	Enabled	SNMP	None		
SG300-CF2-12	Items 367	Triggers 179	Graphs 39	Discovery 6	Web	10.200.99.132-161		Cisco ICS versions 12.0_3_T-12.2_3.5 by SNMP	Enabled	SNMP	None		
SG300-CF3-12	Items 482	Triggers 222	Graphs 48	Discovery 6	Web	10.200.99.133-161		Cisco ICS versions 12.0_3_T-12.2_3.5 by SNMP	Enabled	SNMP	None		
SG300-CF4-12	Items 23	Triggers 10	Graphs 1	Discovery 5	Web	10.200.99.134-161		Cisco ICS prior to 12.0_3_T by SNMP	Enabled	SNMP	None		

ภาพที่ 4.60 การแสดงข้อมูลในหน้าแสดงข้อมูลของอุปกรณ์ทั้งหมดที่มีในระบบ

ขั้นตอนที่ 7 รายงานและสรุปผล

1. การปรับปรุงระบบตามงบประมาณที่ได้รับเป็นไปตามแผนและผ่านการอนุมัติจากผู้บริหาร
2. การดำเนินงานมีขั้นตอนชัดเจนตาม Activity Diagram ทำให้สามารถควบคุมกระบวนการได้อย่างมีประสิทธิภาพ
3. การติดตั้งอุปกรณ์ใหม่ช่วยเพิ่มความเร็วและความเสถียรของระบบเครือข่ายภายในสถาบัน
4. ระบบ Monitoring ช่วยเฝ้าติดตามและบริหารจัดการอุปกรณ์ได้อย่างมีประสิทธิภาพ
5. การทดสอบและตรวจสอบก่อนส่งมอบช่วยลดความผิดพลาดในการใช้งานจริง
6. ผลการปรับปรุงช่วยส่งเสริมการปฏิบัติงานของบุคลากรและการเรียนการสอนของนักศึกษาได้อย่างต่อเนื่อง

4.4 วิธีการติดตามประเมินผลการปฏิบัติงาน

เพื่อให้การดำเนินงานด้านการออกแบบและจัดการระบบเครือข่ายคอมพิวเตอร์ของสถาบันดนตรีก็ลายาณิวัฒนามีประสิทธิภาพ มีความโปร่งใส ตรวจสอบได้ และสามารถปรับปรุงพัฒนาอย่างต่อเนื่อง ผู้บังคับบัญชาหรือผู้มีอำนาจหน้าที่ที่เกี่ยวข้อง จะดำเนินการติดตามและประเมินผลการปฏิบัติงานตามแนวทางดังนี้:

1. การติดตามผลการดำเนินงาน

1.1 ติดตามตามแผนงานและระยะเวลา (Time-Based Monitoring) ตรวจสอบการดำเนินงานในแต่ละกิจกรรมตามระยะเวลาที่กำหนดในแผนงานใช้เอกสารประกอบ เช่น ตารางกิจกรรม, แผน Gantt Chart หรือปฏิทินปฏิบัติงาน เพื่อเปรียบเทียบกับการดำเนินงานจริง

1.2 การรายงานความก้าวหน้าเป็นระยะ (Progress Report) ผู้รับผิดชอบโครงการต้องจัดทำรายงานความก้าวหน้ารายสัปดาห์หรือรายเดือน ส่งให้ผู้บังคับบัญชาพิจารณาในกรณีพบปัญหาหรืออุปสรรค จะต้องแนบแนวทางแก้ไขและผลกระทบที่อาจเกิดขึ้น

1.3 การตรวจพื้นที่หน้างาน (Site Inspection) ผู้บังคับบัญชาหรือผู้แทนสามารถลงพื้นที่เพื่อตรวจสอบความเรียบร้อยของงานติดตั้งอุปกรณ์ตรวจสอบความถูกต้องตามแผนผังเครือข่าย จุดเชื่อมต่อ สายสัญญาณ และความเรียบร้อยของระบบ

2. วิธีการประเมินผลการปฏิบัติงาน

2.1 การประเมินผลตามตัวชี้วัด (KPI – Key Performance Indicators) ประเมินจากเกณฑ์ที่กำหนด เช่น ดำเนินงานเสร็จภายในเวลาที่กำหนด อุปกรณ์ติดตั้งครบถ้วนตามแผนระบบสามารถใช้งานได้โดยไม่มีปัญหาสำคัญความพึงพอใจของผู้ใช้งาน (แบบสอบถาม)

2.2 การทดสอบระบบหลังติดตั้ง (System Acceptance Testing) ประเมินคุณภาพของระบบจากการทดสอบการเชื่อมต่อ ความเร็ว และความเสถียร ตรวจสอบว่า VLAN, IP, การกำหนดสิทธิ์ และการเข้าใช้งานเป็นไปตามมาตรฐานที่วางไว้

2.3 การวิเคราะห์และสรุปผลการดำเนินงาน (Post-Project Evaluation) ผู้รับผิดชอบโครงการต้องจัดทำรายงานสรุปผลการดำเนินงาน พร้อมแสดงจุดแข็ง จุดอ่อน และข้อเสนอแนะเพื่อปรับปรุงผู้บังคับบัญชาทบทวนผลลัพธ์ เปรียบเทียบกับเป้าหมายที่กำหนด และพิจารณาปรับปรุงขั้นตอนในรอบถัดไป

3. เครื่องมือ/ช่องทางที่ใช้ในการติดตามและประเมิน

1. แบบฟอร์มรายงานประจำขั้นตอน เช่น รายงานสำรวจพื้นที่ รายงานการติดตั้ง รายงานทดสอบ
2. แบบฟอร์มประเมินตนเองของเจ้าหน้าที่ (Self-assessment Form)
3. แบบสอบถามความพึงพอใจของผู้ใช้งาน (User Feedback Form)
4. ระบบติดตามผลผ่านแอปหรือระบบออนไลน์ เช่น Google Sheets, ระบบ Intranet ภายในหน่วยงาน
5. ประชุมสรุปผล (Debriefing Meeting) หลังโครงการเพื่อรับฟังความคิดเห็นจากทีมงาน

4.5 จรรยาบรรณ/คุณธรรม/จริยธรรมในการปฏิบัติงาน

1. ต้องมีความซื่อสัตย์ทางวิชาชีพ ไม่นำผลงานของผู้อื่นมาเป็นผลงานของตน ไม่ใช่หรืออ้างงานผู้อื่นให้ทำ ผลงานและนำไปใช้ในการเสนอขอตำแหน่ง และไม่ลอกเลียนผลงานของผู้อื่น รวมทั้งไม่นำผลงานของตนเองในเรื่องเดียวกันไปเผยแพร่ในวารสารวิชาการหรือวิชาชีพมากกว่าหนึ่งฉบับในลักษณะที่จะทำให้เข้าใจผิดว่าเป็นผลงานใหม่
2. ต้องให้เกียรติและอ้างถึงบุคคลหรือแหล่งที่มาของข้อมูลที่นำมาใช้ในผลงานทางวิชาชีพของตนเองและแสดงหลักฐานของการค้นคว้า
3. ต้องไม่คำนึงถึงผลประโยชน์ทางวิชาชีพจนละเลยหรือละเมิดสิทธิส่วนบุคคลของผู้อื่นและสิทธิมนุษยชน
4. ผลงานทางวิชาชีพต้องได้มาจากการศึกษาโดยใช้หลักวิชาชีพเป็นเกณฑ์ ไม่มีอคติมาเกี่ยวข้อง และ เสนอผลงานตามความเป็นจริง ไม่จงใจเบี่ยงเบนผลการศึกษา วิเคราะห์ สังเคราะห์ หรือวิจัยโดยหวัง ผลประโยชน์ส่วนตัว หรือต้องการสร้างความเสียหายแก่ผู้อื่น และเสนอผลงานตามความเป็นจริง ไม่ขยายข้อค้นพบโดยปราศจากการตรวจสอบยืนยันในทางวิชาชีพ
5. ต้องนำผลงานไปใช้ประโยชน์ในทางที่ชอบธรรม และชอบด้วยกฎหมาย
6. หากผลงานทางวิชาชีพมีการใช้ข้อมูลจากการทำการวิจัยในคนหรือสัตว์

บทที่ 5

ปัญหาอุปสรรค และแนวทางในการแก้ไขและการพัฒนางาน

เพื่อให้การดำเนินงานออกแบบและจัดการระบบเครือข่ายของสถาบันดนตรีกัลยาณีวัฒนา มีประสิทธิภาพสูงสุด การระบุปัญหา อุปสรรค และแนวทางแก้ไขอย่างเป็นระบบจึงเป็นสิ่งจำเป็น โดยพิจารณาจากแต่ละขั้นตอนในกระบวนการติดตั้งและทดสอบระบบตามแผนภาพ ดังนี้:

5.1 ปัญหาอุปสรรคในการปฏิบัติงาน

ขั้นตอน: สำรวจพื้นที่ที่ติดตั้ง

ปัญหา: ข้อมูลหน้างานไม่ครบถ้วน พื้นที่จริงมีข้อจำกัด เช่น ความสูงของฝ้า หรือไม่มีช่องทางเดินสาย

ขั้นตอน: ออกแบบการติดตั้ง

ปัญหา: ออกแบบไม่ครอบคลุมอุปกรณ์หรือความต้องการในอนาคต เช่น การขยายพื้นที่ใช้งาน

ขั้นตอน: บันทึกข้อความแจ้งเพื่อขอดำเนินการติดตั้ง

ปัญหา: ล่าช้าในการจัดทำเอกสารหรือไม่ได้รับการอนุมัติทันเวลา

ขั้นตอน: เสนอผู้บริหารพิจารณาอนุญาต

ปัญหา: ผู้มีอำนาจอนุมัติไม่เข้าใจรายละเอียดทางเทคนิค ทำให้เกิดการปฏิเสธหรือขอเอกสารเพิ่ม

ขั้นตอน: ติดตั้งอุปกรณ์

ปัญหา: ติดตั้งไม่ตรงตามแผนที่วางไว้ เนื่องจากข้อจำกัดหน้างาน หรืออุปกรณ์ล่าช้า

ขั้นตอน: ทดสอบการใช้งาน

ปัญหา: ระบบไม่ผ่านการทดสอบ เช่น ความเร็วไม่ถึงหรือการกระจายสัญญาณ Wi-Fi ไม่ทั่วถึง

ขั้นตอน: รายงานและสรุปผล

ปัญหา: รายงานไม่ครบถ้วน หรือไม่มีการวิเคราะห์เปรียบเทียบกับแผนที่กำหนดไว้

5.2 แนวทางในการแก้ไขและพัฒนา

ขั้นตอน: สำรวจพื้นที่ที่ติดตั้ง

แนวทางแก้ไข: จัดทำแบบฟอร์มสำรวจพื้นที่อย่างเป็นระบบ และให้ทีมงานสำรวจลงพื้นที่จริง ร่วมกับเจ้าหน้าที่ของอาคาร

แนวทางพัฒนา: ใช้เทคโนโลยีเช่นการสแกนแผนที่ด้วย Lidar หรือกล้อง 360° เพื่อเก็บข้อมูลพื้นที่อย่างละเอียด

ขั้นตอน: ออกแบบการติดตั้ง

แนวทางแก้ไข: วิเคราะห์ความต้องการของผู้ใช้ทั้งในปัจจุบันและอนาคต รวมถึงเพื่อความสามารถในการขยายเครือข่าย (Scalability)

แนวทางพัฒนา: จัดทำแบบจำลองจำลอง 3D หรือ Simulation ก่อนลงมือจริง เพื่อลดข้อผิดพลาดในการออกแบบ

ขั้นตอน: บันทึกข้อความแจ้งเพื่อขอดำเนินการติดตั้ง

แนวทางแก้ไข: จัดทำเอกสารล่วงหน้าและเตรียมลายเซ็นผู้เกี่ยวข้องให้พร้อมก่อนถึงขั้นตอนนี้

แนวทางพัฒนา: พัฒนาแบบฟอร์มออนไลน์ และระบบติดตามสถานะคำร้องผ่านระบบดิจิทัล (e-Document Tracking)

ขั้นตอน: เสนอผู้บริหารพิจารณาอนุญาต

แนวทางแก้ไข: แบนสรุปเชิงเทคนิคฉบับย่อและผลกระทบกรณีไม่ได้ดำเนินการ เพื่อประกอบการตัดสินใจ

แนวทางพัฒนา: จัดทำ “Executive Summary” ทุกโครงการ พร้อม Infographic หรือภาพประกอบเข้าใจง่าย

ขั้นตอน: ติดตั้งอุปกรณ์

แนวทางแก้ไข: ให้ทีมช่างประชุมกับผู้ออกแบบก่อนดำเนินการติดตั้ง และมีแผนสำรองหากมีอุปกรณ์ล่าช้า

แนวทางพัฒนา: ใช้ระบบ QR Code ติดอุปกรณ์เพื่อติดตามสถานะ และจัดเก็บคู่มือไว้ในระบบออนไลน์

ขั้นตอน: ทดสอบการใช้งาน

แนวทางแก้ไข: ปรับปรุงค่าคอนฟิก ตรวจสอบจุดกระจายสัญญาณ และทดสอบซ้ำ

แนวทางพัฒนา: จัดทำ Checklist มาตรฐาน และบันทึกผลการทดสอบทุกจุดในระบบฐานข้อมูลเพื่อตรวจสอบย้อนหลัง

ขั้นตอน: รายงานและสรุปผล

ปัญหา: รายงานไม่ครบถ้วน หรือไม่มีการวิเคราะห์เปรียบเทียบกับแผนที่กำหนดไว้

แนวทางแก้ไข: กำหนดแบบฟอร์มรายงานมาตรฐาน พร้อม Checkpoint การดำเนินการจริงเทียบกับแผน

แนวทางพัฒนา: ใช้ระบบออนไลน์ในการจัดทำรายงาน พร้อมภาพประกอบและผลการตรวจวัดแบบอัตโนมัติ

5.3 ข้อเสนอแนะ

พัฒนาคู่มือการทำงานที่มีรายละเอียดในแต่ละขั้นตอนย่อย พร้อมแบบฟอร์มและตัวอย่างการกรอกฟอร์มเจ้าหน้าที่ให้เข้าใจบทบาทในแต่ละขั้นตอน และสามารถตัดสินใจแก้ไขหน้างานได้อย่างมีประสิทธิภาพสร้างระบบฐานข้อมูลกลาง (Network Asset Database) สำหรับบันทึกอุปกรณ์สถานะ และการบำรุงรักษาใช้ซอฟต์แวร์ Network Management Tool เพื่อติดตามการติดตั้งทดสอบ และแจ้งเตือนปัญหาผ่านระบบเดียว

บรรณานุกรม

บทความ 3 Tier Design Architecture. สืบค้นจาก <https://www.nsc-corp.co.th/articles/3-tier-design-architecture->

บทความ VLAN คืออะไร? มีประโยชน์อย่างไร? มาทำความรู้จักกันแบบง่ายๆกัน. สืบค้นจาก <https://www.ablenet.co.th/2023/05/02/what-is-vlan/>

บทความ ความสำคัญของการออกแบบระบบเครือข่ายให้มีประสิทธิภาพ สำหรับ โรงเรียน และ มหาวิทยาลัย. สืบค้นจาก <https://nt-metro-service.com/article/network-design/>

บทความ VLAN (Virtual LAN) คืออะไร. สืบค้นจาก [https://www.comebuy.co.th/รายละเอียด/VLAN_Und_\(Virtual_Und_LAN\)_Und_คืออะไร](https://www.comebuy.co.th/รายละเอียด/VLAN_Und_(Virtual_Und_LAN)_Und_คืออะไร)

บทความ Subnet Mask คืออะไร. สืบค้นจาก <https://itbolt.blogspot.com/2017/08/subnet-mask.html>

บทความ มาทำความรู้จักกับ IP Address ทั้ง 2 Versions ที่ใช้ในปัจจุบันกันเถอะ. สืบค้นจาก <https://www.commtech.co.th/blogs/ip-address-2-versions>

บทความ วิธีการแบ่ง Subnet ของเครือข่ายนั้นๆ — subnetting วิชา Network. สืบค้นจาก <https://piravit.medium.com/วิธีการแบ่ง-subnet-ของเครือข่ายนั้นๆ-subnetting-วิชา-network-561c855ef586>

Cisco SG300 CLI Commands. สืบค้นจาก <https://navarajthapa.com.np/cisco-sg300-cli-commands/>

VLAN Configuration via CLI on 300/500 Series Managed Switches. สืบค้นจาก <https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb4986-vlan-configuration-via-cli-on-300-500-series-managed-switches.html>

ประวัติผู้เขียน

ชื่อ-สกุล	พงศธร ศรีวิเศษ
สถานที่เกิด	จังหวัดยโสธร
ที่อยู่ปัจจุบัน	อำเภอพุทธมณฑล จ.นครปฐม 73170
สถานที่ทำงาน	งานเทคโนโลยีและสารสนเทศ สำนักงานสถาบัน สถาบันดนตรีกัลยาณี วัฒนา

ประวัติการศึกษา

พ.ศ. 2550	ปริญญาตรี สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
-----------	---

ประสบการณ์ทำงาน

พ.ศ. 2551	ตำแหน่ง นักวิชาการคอมพิวเตอร์ สำนักวิทยบริการ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ วิทยาเขตศาลายา
พ.ศ. 2552	ตำแหน่ง นักวิชาการสารสนเทศ วิทยาลัยดุริยางคศิลป์ มหาวิทยาลัยมหิดล
พ.ศ. 2556	ตำแหน่ง โปรแกรมเมอร์ (Programmer) บริษัท จินตนาอินเตอร์เทรต จำกัด
พ.ศ. 2557	ตำแหน่ง นักวิชาการสารสนเทศ ศูนย์จิตตปัญญาศึกษา มหาวิทยาลัยมหิดล
พ.ศ. 2557	ตำแหน่ง นักเทคโนโลยีคอมพิวเตอร์ สถาบันดนตรีกัลยาณีวัฒนา