รายงานสหกิจศึกษาฉบับสมบูรณ์

POC สำหรับระบบยืนยันตัวตนและระบบจัดการการสื่อสารภายในองค์กร

POC for Authentication Server and Call Manager

นายณัฐพงศ์สิริ นามกุล

สาขาวิชาวิศวกรรมสารสนเทศ ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2562

ชื่อโครงงานสหกิจศึกษา POC สำหรับระบบยืนยันตัวตนและระบบจัดการการสื่อสารภายในองค์กร

ชื่อ-สกุล นักศึกษา นายณัฐพงศ์สิริ นามกุล

คณะ วิศวกรรมศาสตร์ **ภาควิชา** วิศวกรรมคอมพิวเตอร์ **สาขาวิชา** วิศวกรรมสารสนเทศ

ชื่อ-สกุล อาจารย์นิเทศน์ ผศ. มยุรี เลิศเวชกุล

ชื่อ-สกุล ผู้นิเทศน์งาน คุณตฤณ ปฐมนุพงศ์

ชื่อสถานประกอบการ บริษัท โกลบอล เอ็นทีที (ประเทศไทย) จำกัด

บทคัดย่อ

บริษัท โกลบอล เอ็นทีที (ประเทศไทย) จำกัด เป็นบริษัทที่ให้บริการในการจัดการระบบเครือข่ายและมอบโซลูชั่นทางด้านไอทีให้กับธุรกิจของลูกค้า โดยทางบริษัทมีความต้องการนำเสนอแนวทางการวางระบบเครือข่ายให้กับลูกค้ารายหนึ่งในรูปแบบของการจัดทำ POC หรือ Proof of Concept ซึ่งในโครงงานนี้มีวัตถุประสงค์เพื่อออกแบบ POC สำหรับการวางระบบเครือข่ายในธุรกิจขนาดเล็ก ที่มีความต้องการใช้งานการจำกัดสิทธิ์และยืนยันตัวตนในการเข้าถึงระบบเครือข่ายและต้องการจัดทำระบบสื่อสารภายในองค์กร

คำสำคัญ: Proof of Concept, ระบบสื่อสารภายในองค์กร, การจำกัดสิทธิ์และยืนยันตัวตนในการเข้าถึงระบบเครือข่าย

Co-operative Title: POC of Authentication Server and Call Manager

Student Intern Name: Nattapongsiri Narmkul

Faculty: Engineering **Department:** Computer Engineering (Informtion Engineering)

Advisor Name: Asst. Prof. Mayuree Lertwatechakul

Mentor Name: Tin Prathomnupong

Company: Global NTT (Thailand) Limited

ABSTRACT

Global NTT (Thailand) Ltd. is the company who provide networking solutions and IT solution to customers. Recently the company wanted to present networking solutions to customer in form of POC or Proof of Concept. This project is to design a POC for a small organization who require secured network access control as well as the internal communication system.

Keywords: Proof of Concept, VoIP, Authentication

กิตติกรรมประกาศ

โครงงานการจัดทำ POC สำหรับทดสอบระบบยืนยันตัวตนภายและระบบการสื่อสารภายในองค์กรนี้เป็นหัวข้อโครงงานในโครงการสหกิจศึกษาที่เป็นความร่วมมือระหว่างบริษัท ไดเมนชั่น ดาต้า (ประเทศไทย) จำกัด กับสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง โดยมีระยะเวลาในการปฏิบัติงานของนักศึกษาตั้งแต่วันที่ 5 สิงหาคม 2562 ถึงวันที่ 29 พฤศจิกายน 2562 โดยในระหว่างปฏิบัติงานให้กับทางบริษัทนั้น ได้มีการสนับสนุนและความอนุเคราะห์จากผู้มีส่วนเกี่ยวข้องหลายฝ่ายจึงทำให้การปฏิบัติงานและการจัดทำโครงงานเป็นไปอย่างครบถ้วนสมบูรณ์

จึงขอแสดงความขอบคุณแก่ คุณตฤณ ปฐมนุพงศ์ ที่คอยให้ความรู้และคำแนะนำตลอดระยะเวลาการปฏิบัติงานของนักศึกษา และขอแสดงความขอบคุณแก่พนักงานในทีม Support Services ที่คอยให้ความรู้และคำแนะนำอีกทั้งยังคอยดูแลในการปฏิบัติงานให้เป็นไปอย่างราบรื่น

และขอแสดงความขอบคุณเป็นอย่างสูงต่อ ผศ.มยุรี เลิศเวชกุล อาจารย์ที่ปรึกษาในโครงการสหกิจศึกษา ที่คอยให้คำแนะนำในการจัดทำโครงงาน อีกทั้งยังช่วยตรวจสอบและเสนอแนะแนวทางในการปรับปรุงแก้ไขเนื้อหาของโครงงานให้มีความสมบูรณ์ จึงทำให้โครงงานนี้สำเร็จลุล่วงไปด้วยดี

ณัฐพงศ์สิริ นามกุล

สารบัญ

บทที่ **หน้า**

บทคัดย่อ I

ABSTRACT II

กิตติกรรมประกาศ III

สารบัญ IV

สารบัญภาพ VII

สารบัญตาราง XII

บทที่ 1 บทนำ 1

1.1 ที่มาและความสำคัญ 1

1.2 วัตถุประสงค์ของโครงงาน 1

1.3 วิธีการดำเนินงาน 2

1.4 ประโยชน์ที่คาดว่าจะได้รับ 2

บทที่ 2 ทฤษฎีและเครื่องมือที่เกี่ยวข้อง 3

2.1 ทฤษฎีที่เกี่ยวข้อง 3

2.1.1. 3-Tier Hierarchical Model 3

2.1.2. Virtual Machine 3

2.1.3. AAA Server 4

2.1.4. RADIUS 4

2.1.5. NTP 5

2.1.6. Active Directory 5

2.1.7. LDAP 5

2.1.8. IP Telephony และ VoIP 5

2.1.9. Partition และ Calling Search Space (CSS) 6

2.2 เครื่องมือที่เกี่ยวข้อง 6

สารบัญ (ต่อ)

บทที่ **หน้า**

2.2.1. Cisco UCS C220 M3 Rack Server 6
2.2.2. Cisco 3504 Wireless LAN Controller 6
2.2.3. Cisco Catalyst 2960-L Series Switch 6
2.2.4. Cisco Aironet 1815 7
2.2.5. Cisco IP Phone 7821 7
2.2.6. External ISP Gateway 7
2.2.7. VMware ESXi 7
2.2.8. Ubuntu 18.04 7
2.2.9. freeRADIUS 8
2.2.10. Windows Server 2016 8
2.2.11. Cisco Unified Communications Manager (CUCM) 8

บทที่ 3 ขั้นตอนการดำเนินงาน 9

3.1 วิเคราะห์และออกแบบระบบเครือข่าย 9
3.2 การศึกษาข้อมูลและจัดเตรียมอุปกรณ์ให้เหมาะสมกับการนำมาใช้ในระบบเครือข่ายจำลอง. 11
3.3 การดำเนินการติดตั้งระบบ 13
3.3.1. ดำเนินการเชื่อมต่ออุปกรณ์ในระบบเครือข่ายจำลอง 13
3.3.2. การจัดเตรียมเครื่อง Cisco UCS C220 M3 Rack Server 14
3.3.3. การติดตั้ง VMware ESXi 14
3.3.4. การตั้งค่าให้ Gateway 18
3.3.5. การสร้าง Network Adapter ภายใน VMware ESXi 18
3.3.6. การสร้าง Guest OS ตัวที่ 1 22
3.3.7. การติดตั้ง Ubuntu Desktop 18.04 25
3.3.8. การติดตั้งส่วนประกอบเพิ่มเติมลงบน Ubuntu 18.04 server 27
3.3.9. การติดตั้ง Wireless LAN Controller (WLC) และ Cisco Access Point 32
3.3.10. การตั้งค่าระบบยืนยันตัวตนผู้เข้าใช้งานระบบเครือข่ายภายในองค์กร 35

สารบัญ (ต่อ)

บทที่ **หน้า**

3.3.11. การกำหนดค่าให้ WLANs ได้มีการเรียกใช้การยืนยันตัวตนกับ RADIUS Server 36

3.3.12. การสร้าง Guest OS ตัวที่ 2 (Active Directory) 37

3.3.13. การติดตั้ง Active Directory 39

3.3.14. การสร้าง Organization Unit และบัญชีผู้ใช้งานมีบทบาทเป็นผู้ดูแลระบบ 46

3.3.15. การสร้าง Guest OS ตัวที่ 3 (Call Manager) 50

3.3.16. การติดตั้งและทดสอบระบบโทรศัพท์ IP Phone 57

3.3.17. การตั้งค่าให้กับ Management และ Access Switch 62

บทที่ 4 ผลการทดลอง 63

4.1 การเข้าใช้งานหน้า CONSOLE ของ UBUNTU 18.04 ผ่านทาง SSH 63

4.2 ทดสอบการเข้าไป CONFIG อุปกรณ์ 65

4.3 ทดสอบการเข้าใช้งานระบบเครือข่าย 66

4.4 ทดสอบการทำงานของ LDAP DIRECTORY 69

4.5 ทดสอบการทำงานของ CUCM 71

บทที่ 5 สรุปผลการดำเนินงาน 79

เอกสารอ้างอิง 80

สารบัญภาพ

รูปที่ **หน้า**

รูปที่ 3.1 NETWORK TOPOLOGY 10

รูปที่ 3.2 หน้าเว็บการจัดการของ CIMC 14

รูปที่ 3.3 การเลือก BOOT DEVICES 15

รูปที่ 3.4 การเลือกไฟล์ติดตั้ง VMWARE ESXI 15

รูปที่ 3.6 การเข้าสู่การตั้งค่าพื้นฐาน VMWARE ESXI 16

รูปที่ 3.7 การเข้าสู่การติดตั้ง VMWARE ESXI 16

รูปที่ 3.8 การตั้งค่า IP ADDRESS สำหรับการเข้าใช้งาน VMWARE ESXI 17

รูปที่ 3.9 หน้าเว็บการจัดการ VMWARE ESXI 17

รูปที่ 3.9 การตั้งค่า LAN 18

รูปที่ 3.10 การเลือกเมนู NETWORKING 19

รูปที่ 3.11 การเพิ่ม STANDARD VIRTUAL SWITCH 1 19

รูปที่ 3.12 การเพิ่ม STANDARD VIRTUAL SWITCH 2 20

รูปที่ 3.13 การเพิ่ม UPLINK ให้กับ VIRTUAL SWITCH 1 20

รูปที่ 3.14 การเพิ่ม UPLINK ให้กับ VIRTUAL SWITCH 2 21

รูปที่ 3.15 การสร้าง PORT GROUP และเพิ่ม VIRTUAL SWITCH ให้ PORT GROUP 21

รูปที่ 3.16 การเลือกสร้าง VM 22

รูปที่ 3.17 การสร้าง VM ขึ้นใหม่ 23

รูปที่ 3.18 การตั้งชื่อและเลือกระบบปฏิบัติการให้กับ VM 23

รูปที่ 3.19 การเลือก STORAGE สำหรับการเก็บข้อมูล 24

รูปที่ 3.20 การเพิ่ม NETWORK ADAPTER ให้กับ VM 25

สารบัญภาพ (ต่อ)

รูปที่ **หน้า**

รูปที่ 3.21 การเลือกติดตั้ง UBUNTU 18.04 แบบ MINIMAL INSTALLATION 26

รูปที่ 3.22 การตั้ง IP ADDRESS ให้กับ SERVER01 26

รูปที่ 3.23 การแสดงผลสถานะการทำงานของ NTP SERVER 27

รูปที่ 3.24 การตั้งค่า NTP POOL ภายในไฟล์ NTP.CONF 28

รูปที่ 3.25 การแสดงผลสถานะการทำงานของ OPENSSH SERVER 29

รูปที่ 3.26 การสร้างการเชื่อมต่อเข้ามายัง SERVER01 ผ่านโปรโตคอล SSH 29

รูปที่ 3.27 การตรวจสอบเวอร์ชั่นของ FREERADIUS ที่ทำการติดตั้งไป 30

รูปที่ 3.28 การตั้งค่าภายในไฟล์ RADIUSD.CONF 30

รูปที่ 3.29 การเพิ่ม CLIENTS ให้กับ FREERADIUS 31

รูปที่ 3.30 การตั้งค่าการทำงานของ DHCP SERVER 32

รูปที่ 3.31 หน้าเว็บการจัดการของ WLC 1 33

รูปที่ 3.32 หน้าเว็บการจัดการของ WLC 2 33

รูปที่ 3.33 การเพิ่ม NTP SERVER บน WLC 34

รูปที่ 3.34 หน้าการจัดการ AP ที่มีการเชื่อมต่อเข้ามา 34

รูปที่ 3.35 การเพิ่ม RADIUS AUTHENTICATION SERVER ภายใน WLC 1 35

รูปที่ 3.36 การเพิ่ม RADIUS AUTHENTICATION SERVER ภายใน WLC 2 35

รูปที่ 3.37 การเพิ่ม RADIUS ACCOUNTING SERVER ภายใน WLC 36

รูปที่ 3.38 การเปิดใช้งาน RADIUS SERVER ภายใน WLANS 36

รูปที่ 3.39 การตั้งค่าให้ WLANS เรียกใช้งาน DHCP SERVER 37

รูปที่ 3.40 การเลือกติดตั้ง WINDOWS SERVER 2016 DESKTOP EXPERIENCE 38

สารบัญภาพ (ต่อ)

รูปที่ **หน้า**

รูปที่ 3.41 การตั้งค่า ADMINISTRATOR PASSWORD 38

รูปที่ 3.42 การตั้งค่า IP ADDRESS ให้กับ WINDOWS SERVER 39

รูปที่ 3.62 การเลือกติดตั้ง CUCM 50

รูปที่ 3.63 การตั้ค่า TIMEZONE CONFIGURATION 51

รูปที่ 3.64 การตั้งค่า MTU CONFIGURATION 52

รูปที่ 3.65 การตั้งค่า DHCP CONFIGUARTION 52

รูปที่ 3.66 การตั้งค่า NETWORK CONFIGURATION 52

รูปที่ 3.67 การตั้งค่า DNS CLIENT CONFIGURATION 53

รูปที่ 3.68 การตั้งค่า ADMINISTRATOR LOGIN 53

รูปที่ 3.70 การตั้งค่า NTP CLIENT CONFIGURATION 54

รูปที่ 3.71 การตั้งค่า SECURITY PASSWORD 54

รูปที่ 3.72 การกำหนด SMART CALL HOME 54

รูปที่ 3.73 การตั้งค่า APPLICATION USER 55

รูปที่ 3.74 หน้าจอแสดงผลว่าการตั้งค่าเสร็จสมบูรณ์พร้อมทำการติดตั้งต่อ 55

รูปที่ 3.75 การ LOGIN เข้าใช้งาน CUCM ผ่านหน้า CONSOLE 56

รูปที่ 3.76 การเข้าใช้งาน CUCM ผ่านหน้าเว็บ 1 56

รูปที่ 3.77 การเข้าใช้งาน CUCM ผ่านหน้าเว็บ 2 57

รูปที่ 3.78 การเปิดใช้งาน LDAP SYSTEMS 1 57

รูปที่ 3.79 การเปิดใช้งาน LDAP SYSTEMS 2 58

รูปที่ 3.80 การสร้าง LDAP DIRECTORY 1 58

สารบัญภาพ (ต่อ)

รูปที่ **หน้า**

รูปที่ 3.81 การสร้าง LDAP DIRECTORY 2 59

รูปที่ 3.82 การตั้งค่า LDAP DIRECTORY 1 59

รูปที่ 3.83 การตั้งค่า LDAP DIRECTORY 2 60

รูปที่ 3.84 การเข้าสู่ SERVICE ACTIVATION 60

รูปที่ 3.85 การเปิดใช้งาน CISCO DIRSYNC 61

รูปที่ 3.86 การแจ้งเตือนเพื่อไปใช้งาน SERVICES อื่นๆที่เกี่ยวข้อง 61

รูปที่ 3.87 การเปิดใช้งาน CISCO TFTP 62

รูปที่ 4.1 การเชื่อมต่อ IP 172.18.173.26 ผ่านโปรโตคอล SSH 63

รูปที่ 4.2 การ LOGIN เข้าใช้งานด้วย HOSTNAME ของเครื่อง UBUNTU 64

รูปที่ 4.3 การเข้าใช้งานหน้า CONSOLE ของ UBUNTU 64

รูปที่ 4.4 การ LOGIN เข้าใช้งานด้วยบัญชีผู้ใช้งานใน RADIUS SERVER 65

รูปที่ 4.5 LOG แสดงการเข้าถึงของผู้ใช้งานที่เข้ามา CONFIG อุปกรณ์ 65

รูปที่ 4.6 การ LOGIN ด้วยบัญชีผู้ใช้งานที่มีอยู่ใน RADIUS SERVER โดยที่ RADIUS SERVER หยุดการทำงาน 66

รูปที่ 4.7 การ LOGIN ด้วยบัญชี LOCAL ADMIN ของอุปกรณ์ 66

รูปที่ 4.8 การเชื่อมต่อเครือข่ายโดยใช้บัญชีผู้ใช้งานใน RADIUS SERVER (เชื่อมต่อจากคอมพิวเตอร์) 67

รูปที่ 4.9 การเชื่อมต่อเครือข่ายโดยสำเร็จ (เชื่อมต่อจากคอมพิวเตอร์) 67

รูปที่ 4.10 การเชื่อมต่อเครือข่ายโดยใช้บัญชีผู้ใช้งานใน RADIUS SERVER (เชื่อมต่อจากโทรศัพท์) 68

รูปที่ 4.11 การเชื่อมต่อเครือข่ายสำเร็จ (เชื่อมต่อจากโทรศัพท์) 68

รูปที่ 4.12 การแสดงผล LOG ภายใน RADIUS SERVER 69

สารบัญภาพ (ต่อ)

รูปที่ **หน้า**

รูปที่ 4.13 การทำการดึงข้อมูลจาก ACTIVE DIRECTORY 70

รูปที่ 4.14 รายชื่อบัญชีผู้ใช้งานที่ถูกเพิ่มเข้ามาจาก ACTIVE DIRECTORY 70

รูปที่ 4.15 การเพิ่มโทรศัพท์เข้าสู่ CUCM 71

รูปที่ 4.16 การเลือกรุ่นของโทรศัพท์ที่ต้องการ 72

รูปที่ 4.17 การตั้งค่าให้กับโทรศัพท์ 1 72

รูปที่ 4.18 การตั้งค่าให้กับโทรศัพท์ 2 73

รูปที่ 4.19 รายชื่อโทรศัพท์ที่ถูกเพิ่มเข้ามาใน CUCM 73

รูปที่ 4.20 การสร้าง PARTITION 74

รูปที่ 4.21 รายชื่อ PARTITION ที่ถูกสร้างไว้ 74

รูปที่ 4.22 การสร้าง CSS และการเพิ่ม PARTITION เข้าสู่ CSS 75

รูปที่ 4.23 การเพิ่มหมายเลขโทรศัพท์ 1 76

รูปที่ 4.24 การเพิ่มหมายเลขโทรศัพท์ 2 76

รูปที่ 4.25 การเพิ่ม PARTITION และ CSS ให้กับโทรศัพท์ 77

สารบัญตาราง

ตารางที่ 3.1 NETWORK EQUIPMENT และการใช้งาน 11

ตารางที่ 3.1 NETWORK EQUIPMENT และการใช้งาน (ต่อ) 12

ตารางที่ 3.2 ซอฟต์แวร์และการใช้งาน 12

ตารางที่ 3.2 ซอฟต์แวร์และการใช้งาน (ต่อ) 13

ตารางที่ 3.3 IP ADDRESS ของอุปกรณ์ในระบบเครือข่ายจำลอง 13

ตารางที่ 3.3 IP ADDRESS ของอุปกรณ์ในระบบเครือข่ายจำลอง (ต่อ) 14

ตารางที่ 3.4 HARDWARE SETTINGS ของ GUEST OS ตัวที่ 1 24

ตารางที่ 3.5 HARDWARE SETTINGS ของ GUEST OS ตัวที่ 2 37

ตารางที่ 4.1 ข้อมูลและหมายเลขโทรศัพท์สำหรับใช้ในการทดสอบ 77

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญ

บริษัท Global NTT (ประเทศไทย) จำกัด ได้มีการจัดทำโครงการสหกิจศึกษาร่วมกับสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง โดยทางบริษัทได้มีการมอบหมายโครงงานให้นักศึกษาได้ทำการศึกษาและดำเนินงานในส่วนการออกแบบและติดตั้งระบบเครือข่ายจำลอง POC (Proof of Concept) สำหรับใช้ทดสอบการทำงานกับระบบเครือข่ายภายในองค์กรของลูกค้าที่มีความต้องการใช้งานระบบการยืนยันตัวตนเพื่อใช้จำกัดสิทธิ์ในการเข้าถึงเครือข่ายภายในองค์กร(Authentication Server)และการใช้งานระบบการสื่อสารภายในองค์กร(Call Manager) โดยได้มีการมอบหมายงานให้นักศึกษาจัดทำโดยคำนึงถึงความต้องการของลูกค้าเป็นหลัก

ซึ่งการจัดทำ POC เป็นการออกแบบ ทดสอบ และติดตั้งระบบเครือข่ายจำลองไว้ภายในแลปเพื่อใช้เป็นระบบตัวอย่างสำหรับการทดสอบการทำงานต่างๆและใช้ในการสร้างความเชื่อมั่นให้กับลูกค้าว่าระบบเครือข่ายที่มีการออกแบบมานั้นสามารถนำไปใช้งานได้จริงและตรงตามความต้องการของลูกค้าก่อนที่ลูกค้าจะให้การยืนยันที่จะนำระบบเครือข่ายไปติดตั้งในพื้นที่จริง และเมื่อติดตั้งระบบจริงในพื้นที่ของลูกค้าแล้วระบบจำลอง POC นี้ ก็อาจนำไปปรับใช้เป็นระบบจำลองสำหรับทำการทดสอบการแก้ไขหรือเปลี่ยนแปลงการทำงานในระบบและสังเกตผลที่เกิดขึ้นก่อนดำเนินการกับระบบจริงของลูกค้า เพื่อช่วยเพิ่มความปลอดภัยและป้องกันผลกระทบที่อาจเกิดขึ้นกับระบบของลูกค้า

1.2 วัตถุประสงค์ของโครงงาน

1) ออกแบบและติดตั้งระบบการยืนยันตัวตนสำหรับจำกัดสิทธิ์ในการเข้าถึงเครือข่ายภายในองค์กร (Authentication Server) เพื่อช่วยเพิ่มความปลอดภัยให้กับระบบเครือข่าย
2) ออกแบบและติดตั้งระบบการสื่อสารภายในองค์กรด้วยระบบโทรศัพท์ IP-Phone
3) นำระบบที่ถูกติดตั้งไปใช้นำเสนอกับลูกค้า โดยระบบจำลองจะช่วยอำนวยความสะดวกในการเข้าทดสอบการทำงานต่างๆในระบบแก่ลูกค้า และยังเพิ่มความเชื่อมั่นให้กับลูกค้าว่าระบบที่ออกแบบมานั้นสามารถทำงานได้ตรงตามความต้องการ

1.3 วิธีการดำเนินงาน

1) สำรวจและวิเคราะห์ความต้องการใช้งานระบบเครือข่ายของลูกค้า
2) ออกแบบระบบเครือข่าย โดยเลือกใช้อุปกรณ์และซอฟต์แวร์ให้เหมาะสม
3) ทำการติดตั้งระบบเครือข่ายจำลอง
4) ทดสอบการทำงานของระบบเครือข่ายจำลอง
5) วิเคราะห์ปัญหาและเสนอแนะแนวทางการเพิ่มประสิทธิภาพของระบบเครือข่าย
6) สรุปผลการดำเนินงาน

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1) นักศึกษาได้ความรู้ในการออกแบบและติดตั้งระบบการยืนยันตัวตนในการเข้าถึงระบบเครือข่าย (Authentication Server) รวมถึงการติดตั้งระบบการจัดการการสื่อสาร (Call Manager)
2) ทางบริษัทได้รับการติดตั้งระบบเครือข่ายจำลองที่มีประสิทธิภาพและได้แนวทางในการออกแบบระบบเครือข่ายที่สามารถใช้งานได้ตามความต้องการของลูกค้า
3) เพิ่มความสะดวกแก่ลูกค้าในการทดสอบการทำงาน และสามารถสร้างความเชื่อมั่นแก่ลูกค้าว่าระบบที่ออกแบบมานั้นสามารถใช้งานได้จริง

บทที่ 2
ทฤษฎีและเครื่องมือที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1. 3-Tier Hierarchical Model

เป็นหลักการในการออกแบบระบบเครือข่ายรูปแบบหนึ่ง ซึ่งมีประโยชน์ในเรื่องของการลดความซับซ้อนในระบบ ทำให้สามารถจัดการได้ง่าย เนื่องจาก จะทำการแยกส่วนการทำงานของส่วนประกอบต่างๆในระบบได้ค่อนข้างชัดเจน โดยจะทำการแบ่งออกเป็น 3 ลำดับชั้น ได้แก่

1) Core Layer เป็นลำดับชั้นที่สูงที่สุด ทำหน้าที่ในการรับส่งข้อมูลไปยังชั้น Distribution Layer โดยอุปกรณ์ที่อยู่ใน Core Layer ควรจะต้องเป็นอุปกรณ์
2) Distribution Layer ทำหน้าที่ในการจำกัดและแยกแยะการส่งข้อมูลจากชั้น Core Layer ไปยัง Access Layer เพื่อไม่ให้ Core Layer รับภาระที่หนักเกินไป
3) Access Layer เป็นลำดับชั้นที่อยู่ต่ำสุดและอยู่ใกล้กับผู้ใช้งานมากที่สุด เพราะเป็นชั้นที่ทำหน้าที่ในการรับส่งข้อมูลจากอุปกรณ์ที่จุดปลายสายนั่นเอง

เมื่อมีการแบ่งการทำงานที่ชัดเจนเป็นลำดับชั้นแล้ว ก็จะทำให้สามารถปรับปรุงแก้ไขอุปกรณ์ในระบบได้ง่ายขึ้น เช่น ถ้าหากอุปกรณ์ในชั้นล่างเกิดการทำงานผิดพลาดก็จะสามารถทำการแก้ไขได้โดยที่ไม่ส่งผลกระทบกับชั้นที่อยู่สูงขึ้นไป ช่วยให้ลดระยะเวลาในการกู้คืนระบบได้ อีกทั้งยังเป็นการออกแบบที่สามารถขยายขอบเขตของระบบได้ง่าย จึงเหมาะกับการนำมาใช้งานจริง ซึ่งในที่นี้เป็นการปรับใช้งานกับธุรกิจขนาดเล็กจึงสามารถลดทอนการใช้อุปกรณ์ออกไป โดยทำการลดทอนให้เหลือเพียง 2 Layer ทำให้ลดการใช้ต้นทุนในการติดตั้งและลดความซับซ้อนของระบบได้

2.1.2. Virtual Machine

Virtual Machine (VM) คือการจำลองสร้างระบบปฏิบัติการขึ้นมาโดยใช้ซอฟต์แวร์ที่ถูกติดตั้งไว้ในเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็น Host โดยที่ VM ที่ถูกสร้างขึ้นมานั้นมีความสามารถเหมือนกับระบบปฏิบัติการจริง โดยที่ทรัพยากรต่างๆในระบบ เช่น หน่วยความจำ, หน่วยประมวลผล หรือ เนื้อที่ในการจัดเก็บข้อมูลจะถูกกำหนดขึ้นมาโดยแบ่งทรัพยากรมาจากเครื่องที่เป็น Host ดังนั้นการสร้าง VM จึง

เปรียบเสมือนการจำลองเครื่องคอมพิวเตอร์อีกเครื่องขึ้นมาภายในเครื่องคอมพิวเตอร์หลักที่ทำหน้าที่เป็น Host นั่นเอง

โดยการใช้งาน VM นั้นมีความหลากหลายในการใช้งานมาก เนื่องจากสามารถจำลองระบบปฏิบัติการได้หลายชนิด ทำให้สามารถปรับใช้งานได้หลายรูปแบบตามความต้องการ และการใช้งาน VM ยังสามารถช่วยลดต้นทุนในการติดตั้งและลดความยุ่งยากในการจัดการได้ โดยใช้ต้นทุนในการติดตั้งเครื่องคอมพิวเตอร์เพียงแค่เครื่องเดียวแล้วทำการติดตั้งซอฟต์แวร์ในการสร้าง VM จากนั้นทำการจำลองระบบปฏิบัติการที่ทำหน้าที่แตกต่างกันไป ก็สามารถใช้งานได้เหมือนกับการติดตั้งเครื่องคอมพิวเตอร์หลายเครื่องแล้ว

2.1.3. AAA Server

AAA Servers ย่อมาจาก Authentication Authorization and Accounting (AAA) เป็นระบบที่สามารถเพิ่มความปลอดภัยให้กับระบบเครือข่ายได้ โดยมีการตรวจสอบสิทธิ์การเข้าถึงของผู้ใช้ (Authentication) ว่าสามารถเข้าถึงระบบเครือข่ายได้หรือไม่ สามารถทำการกำหนดสิทธิ์ในการใช้งาน (Authorization)ให้ผู้ใช้งานแต่ละคนมีสิทธิ์การใช้งานระบบเครือข่ายในระดับที่ต่างกันไป และสามารถตรวจสอบการใช้งานของผู้ใช้งานแต่ละคน (Accounting) เพื่อให้สามารถมองหาการใช้งานที่ผิดปกติได้ จึงเป็นระบบที่ช่วยเพิ่มความปลอดภัยได้เป็นอย่างดี

2.1.4. RADIUS

RADIUS เป็นมาตรฐานหนึ่งในการทำงานของ AAA Servers ที่ช่วยเพิ่มความปลอดภัยให้กับระบบเครือข่าย โดย RADIUS มีองค์ประกอบในการทำงานอยู่ 3 อย่าง ได้แก่

1) Access Clients คือ ผู้ใช้งานที่ต้องการจะเข้าใช้งานระบบเครือข่ายนี้
2) Network Access Servers (NAS) ได้แก่ อุปกรณ์ต่าง ๆ ในระบบ เช่น Switch และ Access Point โดยจะทำหน้าที่ในการส่งผ่านข้อมูลของผู้ใช้งานที่ทำการเชื่อมต่อเข้ามาจาก Access Clients เพื่อไปทำการตรวจสอบสิทธิ์ที่ RADIUS Server ต่อไป
3) RADIUS Server จะรับข้อมูลที่ NAS ส่งมาแล้วทำการตรวจสอบความถูกต้องโดยการเปรียบเทียบกับข้อมูลที่มีอยู่ ก่อนจะส่งผลลัพธ์กลับไปยัง NAS ว่ายินยอมให้เชื่อมต่อเข้ามาหรือไม่เพื่อให้ NAS ทำการเชื่อมต่อหรือตัดการเชื่อมต่อ Access Client นั้น

2.1.5. NTP

NTP หรือ Network Time Protocol เป็นโปรโตคอลที่ใช้สำหรับการ Sync เวลาของอุปกรณ์ในระบบให้ตรงกัน เพื่อไม่ให้เกิดความคลาดเคลื่อนของนาฬิกาในระบบ โดยจะทำการ Sync กันต่อไปในรูปแบบที่เป็นลำดับขั้นซึ่งเรียกว่า Stratum Layer โดยอุปกรณ์ที่อยู่ใน Stratum 1 จะ Sync กับอุปกรณ์ที่อยู่ใน Stratum 0 ซึ่งมีความเที่ยงตรงสูงสุด และอุปกรณ์ใน Stratum 2 ก็จะ Sync กับอุปกรณ์ใน Stratum 1 อีกทีหนึ่ง เป็นต้น โดยในที่นี้จะให้อุปกรณ์ในระบบทำการ Sync กับ NTP Server หลักของประเทศไทยเพื่อให้มีความคลาดเคลื่อนน้อยที่สุด

2.1.6. Active Directory

เป็นบริการในการจัดเก็บข้อมูลในระบบรูปแบบหนึ่ง ซึ่งสามารถเก็บข้อมูลต่างๆของผู้ใช้งานและยังสามารถจัดการกำหนดนโยบายต่างๆให้ผู้ใช้งานในระบบใช้ได้ อีกทั้งยังสามารถใช้เป็นระบบยืนยันตัวตนได้อีกด้วย โดยในที่นี้จะใช้ Active Directory เพื่อใช้เป็นฐานข้อมูลในการจัดเก็บข้อมูลของผู้ใช้งานเพียงอย่างเดียว เพื่อไม่ให้เกิดภาระงานที่หนักเกินไปโดยจะส่งผ่านการยืนยันตัวตนไปยัง RADIUS Server อีกเครื่องหนึ่ง

2.1.7. LDAP

LDAP เป็น Directory Access Protocol รูปแบบหนึ่งที่มีขนาดข้อมูลน้อยลง ทำให้ถูกเรียกว่า Lightweight Directory Access Protocol ซึ่งเป็นโปรโตคอลที่ใช้ในการเข้าถึงข้อมูลภายในฐานข้อมูล เช่น Active Directory โดยทำการกำหนดตำแหน่งของข้อมูลหรือ Entry อย่างเจาะจงเพื่อเป็นเป้าหมายในการให้ผู้ใช้ทำการดึงข้อมูลมาจากฐานข้อมูลของ Server และ Directory ได้อย่างถูกต้อง

2.1.8. IP Telephony และ VoIP

IP Telephony คือระบบการสื่อสารผ่านโปรโตคอล IP ซึ่งหมายถึงการสื่อสารต่างๆทุกรูปแบบ ไม่ว่าจะเป็นการสื่อสารด้วยระบบโทรศัพท์ การสื่อสารด้วย VDO Conference หรือ fax จะทำการติดต่อกันโดยใช้โปรโตคอล IP ผ่านเครือข่าย LAN หรืออินเทอร์เน็ต ส่วน VoIP หรือ Voice over IP จะหมายถึงการสื่อสารในระบบโทรศัพท์ซึ่งหมายถึงการสื่อสารด้วยเสียงเพียงอย่างเดียว โดยการใช้งานระบบการสื่อสารผ่านโปรโตคอล IP นี้ สามารถช่วยลดต้นทุนในการติดตั้งได้เนื่องจากในการวางระบบเครือข่ายส่วนมากจะเป็นการใช้งานผ่านโปรโตคอล IP อยู่แล้วหากใช้งานระบบสื่อสารผ่านโปรโตคอล IP ด้วย ก็จะทำให้ไม่จำเป็นต้องใช้บริการระบบสื่อสารจากภายนอก และยังช่วยให้มีการจัดการระบบได้ง่ายอีกด้วย

2.1.9. Partition และ Calling Search Space (CSS)

เป็นส่วนประกอบหนึ่งในการทำงานของระบบการจัดการการโทรศัพท์ภายใน Cisco Unified Communications Manager (CUCM) ซึ่งทั้ง 2 ส่วนนี้มีการทำงานที่สัมพันธ์กัน โดย Partition เป็นการสร้างรูปแบบของหมายเลขโทรศัพท์เพื่อใช้ในการจำแนกหมายเลขโทรศัพท์ เช่น การแผนกต่างๆในองค์กร ส่วน CSS จะเป็นการรวม Partition ต่างๆเอาไว้ด้วยกันเป็นเสมือนจุดอ้างอิงเพื่อให้โทรศัพท์ในระบบสามารถติดต่อหากันระหว่าง Partition ที่ถูกรวบรวมไว้ใน CSS ได้

2.2 เครื่องมือที่เกี่ยวข้อง

2.2.1. Cisco UCS C220 M3 Rack Server

เป็นผลิตภัณฑ์เครื่อง Server ในตระกูล Unified Computing Systems (UCS) ของทาง Cisco โดยเครื่อง Serverรุ่นนี้มีประสิทธิภาพการทำงานที่สูงพอที่จะสามารถใช้งานกับระบบที่มีการออกแบบมาทั้งในเรื่องของความเร็วการประมวลผล, ขนาดความจุของพื้นที่จัดเก็บข้อมูล และความง่ายในการจัดการ อีกทั้งยังเป็นรุ่นที่มีราคาไม่สูงมากนักจึงเหมาะกับการนำมาใช้เป็นเครื่อง Server ให้กับธุรกิจขนาดเล็กที่มีความจำกัดด้านต้นทุนและต้องการให้ระบบเครือข่ายสามารถทำงานได้อย่างมีประสิทธิภาพ

2.2.2. Cisco 3504 Wireless LAN Controller

เป็นผลิตภัณฑ์ในกลุ่ม Wireless LAN Controller (WLC) ของทาง Cisco ซึ่งเป็นรุ่นที่มีขนาดเล็กเหมาะกับการนำมาใช้ติดตั้งภายในธุรกิจขนาดเล็ก และสามารถรองรับการเชื่อมต่อกับAccess Point ได้ถึง 150 เครื่องและสามารถรองรับจำนวนผู้ใช้งานมากถึง 3000 คน ซึ่งเป็นระดับที่เพียงพอกับความต้องการใช้งานของลูกค้าแล้ว

2.2.3. Cisco Catalyst 2960-L Series Switch

เป็นสวิตช์รุ่นเล็กที่ทาง Cisco ได้มีการออกแบบมาเพื่อให้เกิดความคุ้มค่าในการใช้งานในราคาที่ประหยัดมากขึ้น เนื่องจากสามารถใช้งานฟังก์ชันต่างๆของระบบปฏิบัติการ Cisco IOS ได้อย่างครบถ้วนเทียบเท่ากับสวิตช์ในรุ่นอื่น เช่น สามารถใช้งานโปรโตคอล RADIUS เพื่อเพิ่มความปลอดภัยให้ระบบเครือข่ายได้ อีกทั้งยังสามารถช่วยลดต้นทุนในการติดตั้งสายไฟเพิ่มเติมสำหรับเชื่อมต่อกับอุปกรณ์ปลาย

สายได้ เนื่องจากสวิตช์รุ่นนี้สามารถจ่ายไฟให้กับอุปกรณ์ปลายสายได้ตามมาตรฐานการทำงานของ PoE (Power Over Ethernet) จึงมีความเหมาะสมที่จะนำมาใช้กับระบบที่มีข้อจำกัดในเรื่องต้นทุน

2.2.4. Cisco Aironet 1815

เป็นผลิตภัณฑ์ Wireless Access Point ของทาง Cisco ซึ่งมีความสามารถในการกระจายสัญญาณอย่างครอบคลุม สามารถส่งข้อมูลได้รวดเร็วทำให้เป็นประโยชน์อย่างมากกับผู้ใช้งานในระบบ อีกทั้ง Aironet 1815 นี้ยังมีขนาดและมีรูปทรงที่หลากหลายสามารถนำไปติดตั้งในหลากหลายพื้นที่ และยังมีราคาที่ประหยัดกว่า Access Point รุ่นอื่นของทาง Cisco แต่มีประสิทธิภาพการทำงานใกล้เคียงกัน

2.2.5. Cisco IP Phone 7821

เป็นโทรศัพท์ที่ใช้โปรโตคอล IP ของทาง Cisco ที่สามารถรับการจ่ายไฟผ่านทาง PoE ได้ทำให้ง่ายต่อการติดตั้งและช่วยประหยัดต้นทุนในการติดตั้ง อีกทั้งยังเป็นรุ่นที่มีฟังก์ชันในการทำงานหลากหลายทั้งการโทรผ่านระบบ IP, การรับ-ส่งข้อความ และยังรองรับการจัดการผ่าน Cisco Unified Communications Manager (CUCM) ทำให้ง่ายต่อการจัดการอีกด้วย

2.2.6. External ISP Gateway

เป็นอุปกรณ์ที่ให้บริการโดยผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) จากภายนอกเพื่อให้ระบบเครือข่ายนี้สามารถใช้งานอินเทอร์เน็ตได้

2.2.7. VMware ESXi

เป็นซอฟต์แวร์สำหรับใช้ในการสร้างและจัดการ VM โดย VMware ESXi นั้นสามารถเข้าจัดการจากคอมพิวเตอร์เครื่องอื่นผ่านทางระบบเครือข่ายได้ทำให้มีความสะดวกในการจัดการมากขึ้น โดยสามารถสร้างการทำงานที่หลากหลายภายใน Host เพียงตัวเดียวได้ ทำให้เป็นการประหยัดทรัพยากรและต้นทุนได้ทางหนึ่ง

2.2.8. Ubuntu 18.04

เป็นระบบปฏิบัติการหนึ่งในตระกูล Linux ซึ่งมีประสิทธิภาพในการทำงานและสามารถจัดการได้ง่าย เนื่องจากมีหน้า GUI (Graphics Users Interface) ที่เข้าใจง่าย อีกทั้ง Ubuntu ยังเป็นระบบปฏิบัติการที่ไม่ใช้งานทรัพยากรอย่างสิ้นเปลืองเนื่องจากมีความต้องการของระบบที่ไม่สูงมากนัก และยังสามารถเลือกติดตั้งเฉพาะที่ต้องการใช้งานก็ได้ ซึ่งการใช้งานในโครงงานนี้จะมีการใช้งาน Ubuntu เป็น Authentication Server

2.2.9. freeRADIUS

เป็นซอฟต์แวร์สำหรับติดตั้งเพิ่มเติมเพื่อให้ระบบปฏิบัติการสามารถทำหน้าที่เป็น AAA Servers สำหรับเพิ่มความปลอดภัยให้ระบบเครือข่าย โดย freeRADIUS เป็นซอฟต์แวร์ Open Source ที่สามารถใช้งานได้ฟรี และสามารถทำการกำหนดสิทธิ์การเข้าถึงและยืนยันตัวตนตามมาตรฐานของ RADIUS

2.2.10. Windows Server 2016

เป็นระบบปฏิบัติการของทาง Microsoft ที่มีฟังก์ชันในการใช้งานอย่างหลากหลาย ตั้งแต่การเก็บข้อมูลต่างๆของUsers ไปจนถึงการกำหนด Policy ที่ใช้ในระบบเครือข่าย ซึ่งภายในโครงงานนี้ได้นำมาปรับใช้ให้ Windows Server 2016 ทำหน้าที่เป็น Active Directory เพื่อทำการเก็บข้อมูลผู้ใช้งานภายในองค์กรของลูกค้า

2.2.11. Cisco Unified Communications Manager (CUCM)

เป็นซอฟต์แวร์สำหรับการจัดการการสื่อสารหลากหลายรูปแบบภายในองค์กร โดยรองรับกับระบบการสื่อสารที่มีผู้ใช้งานตั้งแต่ 150 รายไปจนถึง 1,000 ราย ซึ่งเหมาะกับการนำมาใช้ในโครงงานนี้เพราะสามารถใช้จัดการการสื่อสารในระบบโทรศัพท์ผ่านโปรโตคอล IP ตามที่ออกแบบไว้ได้ และ CUCM ยังมีการออกแบบหน้า GUI ให้ใช้งานง่ายอีกด้วย

บทที่ 3
ขั้นตอนการดำเนินงาน

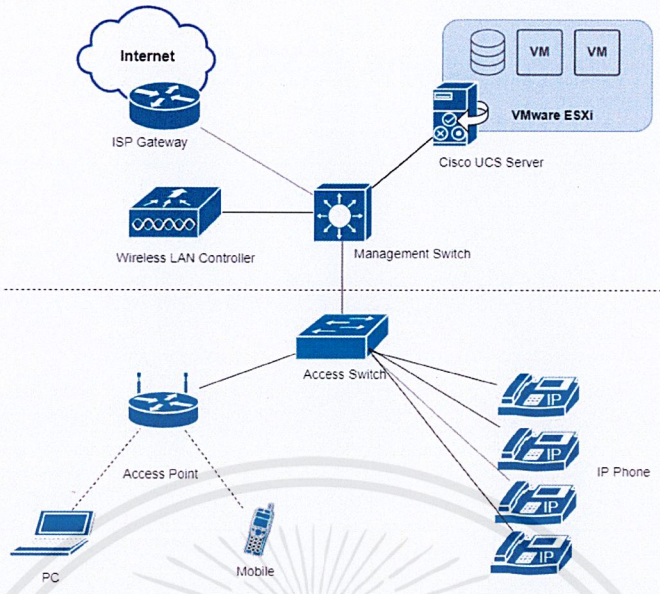
ขั้นตอนการดำเนินงานสามารถแบ่งได้เป็น 3 ขั้นตอน ได้แก่

1) การวิเคราะห์ความต้องการของลูกค้าและออกแบบระบบเครือข่าย
2) การศึกษาข้อมูลและจัดเตรียมอุปกรณ์ให้เหมาะสมกับการนำมาใช้ในระบบเครือข่ายจำลองที่ออกแบบไว้
3) การดำเนินการติดตั้งและทดสอบระบบเครือข่ายจำลอง

3.1 วิเคราะห์และออกแบบระบบเครือข่าย

ในขั้นตอนการวิเคราะห์และออกแบบระบบนั้น ก่อนอื่นต้องทำการรับความต้องการใช้งานระบบของลูกค้ามาทำการวิเคราะห์เพื่อหาแนวทางในการออกแบบระบบให้สามารถทำงานได้ตรงตามความต้องการของลูกค้า โดยจากการสำรวจความต้องการของลูกค้ามานั้นได้ว่าทางลูกค้าต้องการให้ระบบเครือข่ายมีการจำกัดสิทธิ์ในการเข้าใช้งานและสามารถยืนยันตัวตนของผู้ใช้งานได้ และทางลูกค้าต้องการวางระบบการสื่อสารสำหรับใช้ภายในองค์กรอีกด้วย โดยธุรกิจของทางลูกค้านั้นเป็นธุรกิจขนาดเล็กและมีต้นทุนค่อนข้างจำกัด ทางลูกค้าจึงเสนอให้มีการออกแบบโดยคำนึงถึงการใช้ต้นทุนที่มีอย่างจำกัดให้เกิดความคุ้มค่าสูงสุด โดยที่ระบบเครือข่ายสามารถใช้งานได้อย่างมีประสิทธิภาพ

โดยจากการวิเคราะห์ความต้องการของลูกค้าแล้วนั้นจึงได้มีการออกแบบระบบให้เหมาะสมความต้องการใช้งานของลูกค้าตาม Topology ในรูปที่ 3.1



รูปที่ 3.1 Network Topology

จาก Network Topology จะสามารถอธิบายได้ว่าระบบเครือข่ายมีการแบ่งทำงานเป็น 2 ส่วนได้แก่

- Wireless Network สำหรับรองรับการเชื่อมต่อเข้ามาใช้งานระบบเครือข่าย โดยให้ผู้ใช้งานเชื่อมต่อเข้ามาผ่านทาง Access Point ซึ่งผู้ใช้งานที่สามารถใช้งานระบบเครือข่ายได้นั้นต้องมีสิทธิ์ในการเข้าใช้งานและผ่านการยืนยันตัวตนกับ Server ก่อน
- IP Phone Network คือ ระบบโทรศัพท์ผ่านโปรโตคอล IP ที่จะใช้เป็นระบบการสื่อสารหลักภายในองค์กร โดยระบบโทรศัพท์ผ่านโปรโตคอล IP นั้น เป็นระบบการสื่อสารที่มีประสิทธิภาพ สามารถบริหารจัดการได้ง่าย และเป็นระบบการสื่อสารที่ใช้ต้นทุนในการติดตั้งต่ำอีกด้วย

โดยในการออกแบบระบบนั้นได้นำหลักการของ 3-Tier Hierarchical Model มาปรับใช้ให้เหมาะสมกับโครงสร้างธุรกิจขนาดเล็กของลูกค้า โดยทำการลดลำดับชั้นของระบบให้เหลือเพียง 2 ชั้นเพื่อเป็นการลดจำนวนอุปกรณ์ในระบบ โดยการออกแบบในรูปแบบนี้จะทำให้ง่ายต่อการบำรุงรักษาและบริหารจัดการส่วนต่างๆในระบบเพราะมีการแบ่งส่วนการทำงานออกเป็นลำดับชั้น โดยในชั้นล่างสุดจะใช้เชื่อมต่ออุปกรณ์ปลายสายที่มีการติดต่อกับผู้ใช้งาน ได้แก่ Access Point และ IP Phone ส่วนในชั้นสูงขึ้นมาจะเป็นอุปกรณ์ที่ควบคุมการทำงานต่างๆ ได้แก่ Server ทำหน้าที่ในการติดตั้งระบบการจัดการต่างๆของระบบเครือข่าย, Wireless LAN Controller ทำหน้าที่ในการดูแลและจัดการการทำงานของ Access Point และ Gateway สำหรับใช้ในการเชื่อมต่ออินเทอร์เน็ต

ในส่วนของระบบการจัดการต่างๆในระบบจะถูกติดตั้งไว้ภายในเครื่อง Server โดยใช้หลักการของ Virtual Machine คือเครื่อง Server ทำหน้าที่เป็น Host ที่รองรับการสร้างสร้าง Guest OS ขึ้นมาให้สามารถทำหน้าที่แตกต่างกันตามต้องการ ได้แก่

- การใช้เป็นระบบยืนยันตัวตนในการเข้าใช้งานระบบเครือข่าย (Authentication Server)
- การใช้เป็นระบบจัดการการสื่อสาร (Call Manager)

3.2 การศึกษาข้อมูลและจัดเตรียมอุปกรณ์ให้เหมาะสมกับการนำมาใช้ในระบบเครือข่ายจำลอง

จากการศึกษาข้อมูลของอุปกรณ์เพื่อเลือกใช้งานอุปกรณ์ให้เหมาะสมกับระบบเครือข่ายนั้น สามารถสรุปผลการนำอุปกรณ์ต่างๆไปใช้งานโดยแยกประเภทของอุปกรณ์ออกเป็นส่วนของ Network Equipment และซอฟต์แวร์ ได้ดังตารางที่ 3.1 และ 3.2 ตามลำดับ

ตารางที่ 3.1 Network Equipment และการใช้งาน

อุปกรณ์	การใช้งาน
Cisco UCS C220 M3 Rack Server	ใช้ในการติดตั้งซอฟต์แวร์สำหรับจัดการส่วนต่างๆภายในระบบเครือข่าย
Cisco 3504 Wireless LAN Controller	ใช้ในการจัดการการทำงานของ Access Point ภายในระบบ และควบคุมการกระจายสัญญาณให้ผู้ใช้งานสามารถเชื่อมต่อเข้ามาในระบบได้
Cisco Catalyst 2960-L Series Switch	ใช้เป็น Management Switch และ Access Switch เพื่อเชื่อมต่ออุปกรณ์ในระบบเครือข่ายเข้าด้วยกัน โดย Management Switch จะใช้เชื่อมต่ออุปกรณ์ที่ทำหน้าที่จัดการการทำงานในระบบ ได้แก่ เครื่อง Server, WLC และ Gateway ส่วน Access Switch จะใช้ในการเชื่อมต่อกับอุปกรณ์ปลายสาย คือ Access Point และ IP Phone
Cisco Aironet 1815	ใช้ในการกระจายสัญญาณเพื่อให้ผู้ใช้งานทำการเชื่อมต่อเข้ามาใช้งานระบบเครือข่าย

ตารางที่ 3.1 Network Equipment และการใช้งาน (ต่อ)

อุปกรณ์	การใช้งาน
Cisco IP Phone 7821	ใช้เป็นโทรศัพท์ที่ใช้ติดต่อกันภายในระบบเครือข่าย โดยเชื่อมต่อเข้ากับ Access Switch ให้รับการจ่ายไฟผ่านทาง PoE เพื่อให้ง่ายต่อการติดตั้ง และเชื่อมต่อเข้ากับ Cisco Unified Communications Manager (CUCM) เพื่อให้ง่ายต่อการจัดการมากขึ้น
External ISP Gateway	มีการติดตั้งเพื่อให้ระบบเครือข่ายสามารถใช้งานอินเทอร์เน็ตได้ โดยเข้าถึงอินเทอร์เน็ตผ่านบริการของ ISP จากภายนอก

ตารางที่ 3.2 ซอฟต์แวร์และการใช้งาน

ซอฟต์แวร์	การใช้งาน
VMware ESXi	ใช้สำหรับติดตั้งลงบนเครื่อง Server เพื่อให้เครื่อง Server ทำหน้าที่เป็น Host ตามหลักการของ Virtual Machine เพื่อให้สามารถรองรับการสร้าง Guest OS ที่มีหน้าที่แตกต่างกัน
Ubuntu 18.04	ใช้เป็นระบบปฏิบัติการสำหรับใช้บริหารจัดการระบบยืนยันตัวตนและจำกัดสิทธิ์ในการเข้าถึงระบบเครือข่าย
freeRADIUS	ใช้ติดตั้งไปยัง Ubuntu 18.04 เพื่อให้ทำหน้าที่เป็น AAA Servers สำหรับการจำกัดสิทธิ์การเข้าถึงระบบเครือข่ายและยืนยันตัวตนผู้ใช้งาน โดย freeRADIUS เป็นซอฟต์แวร์ Open Source ที่สามารถใช้งานได้ฟรี สามารถใช้งานง่าย และสามารถทำการกำหนดสิทธิ์การเข้าถึงและยืนยันตัวตนตามมาตรฐานของ RADIUS
Windows Server 2016	ใช้เป็น Active Directory ในการจัดเก็บข้อมูลของผู้ใช้งานเพียงอย่างเดียวเพื่อช่วยลดภาระงานของเครื่อง Server

ตารางที่ 3.2 ซอฟต์แวร์และการใช้งาน (ต่อ)

ซอฟต์แวร์	การใช้งาน
Cisco Unified Communications Manager (CUCM)	ใช้เป็นระบบจัดการการสื่อสารภายในองค์กร เนื่องจาก CUCM เป็นระบบที่สามารถใช้งานได้ง่าย และรองรับการจัดการระบบโทรศัพท์ IP Phone ตามที่มีการออกแบบไว้

3.3 การดำเนินการติดตั้งระบบ

3.3.1. ดำเนินการเชื่อมต่ออุปกรณ์ในระบบเครือข่ายจำลอง

ในขั้นตอนแรกสุดนั้นจะเป็นการดำเนินการติดตั้งอุปกรณ์ต่างๆในระบบเครือข่ายจำลองภายในแลปของทางบริษัท ให้มีการเชื่อมต่อกันตาม Topology ที่ออกแบบไว้ก่อน แล้วจึงทำการเข้าไปตั้งค่าอุปกรณ์แต่ละตัวให้มีการทำงานตามที่ออกแบบไว้ในขั้นตอนต่อไป โดยมีแผนการกำหนด IP Address ตามตารางที่ 3.3

ตารางที่ 3.3 IP Address ของอุปกรณ์ในระบบเครือข่ายจำลอง

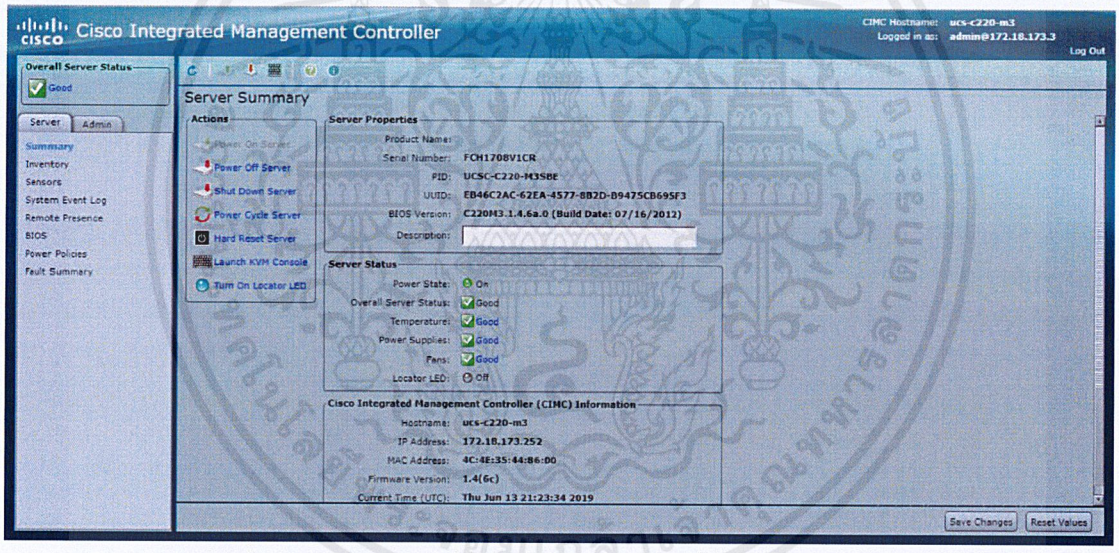
อุปกรณ์/ซอฟต์แวร์	IP Address
Cisco Integrated Management Controller (CIMC)	172.18.173.252
VMware ESXi Hosts	172.18.173.251
Guest OS 1 : Ubuntu (Authentication Server)	172.18.173.26
Guest OS 2 : Windows Server (Active Directory)	172.18.173.27
Guest OS 3 : CUCM (Call Manager)	172.18.173.28
Management Switch	172.18.173.202
Access Switch	172.18.173.201
Cisco WLC	172.18.173.223

ตารางที่ 3.3 IP Address ของอุปกรณ์ในระบบเครือข่ายจำลอง (ต่อ)

อุปกรณ์/ซอฟต์แวร์	IP Address
Cisco AP	172.18.173.23
ISP Gateway	172.18.173.1

3.3.2. การจัดเตรียมเครื่อง Cisco UCS C220 M3 Rack Server

ต้องทำการติดตั้งซอฟต์แวร์ Cisco Integrated Management Controller (CIMC) ซึ่งเป็นซอฟต์แวร์ที่ใช้สำหรับเป็นเครื่องมือในการเข้าถึงและจัดการการทำงานของ Rack Server ทำให้ดูแลและสามารถจัดการการทำงานที่ผิดปกติของ Rack Server ได้สะดวกขึ้นเนื่องจาก CIMC นั้นมีการจัดการผ่านหน้าเว็บที่มีการออกแบบมาให้ใช้งานง่าย โดยมีหน้าตาดังรูปที่ 3.2

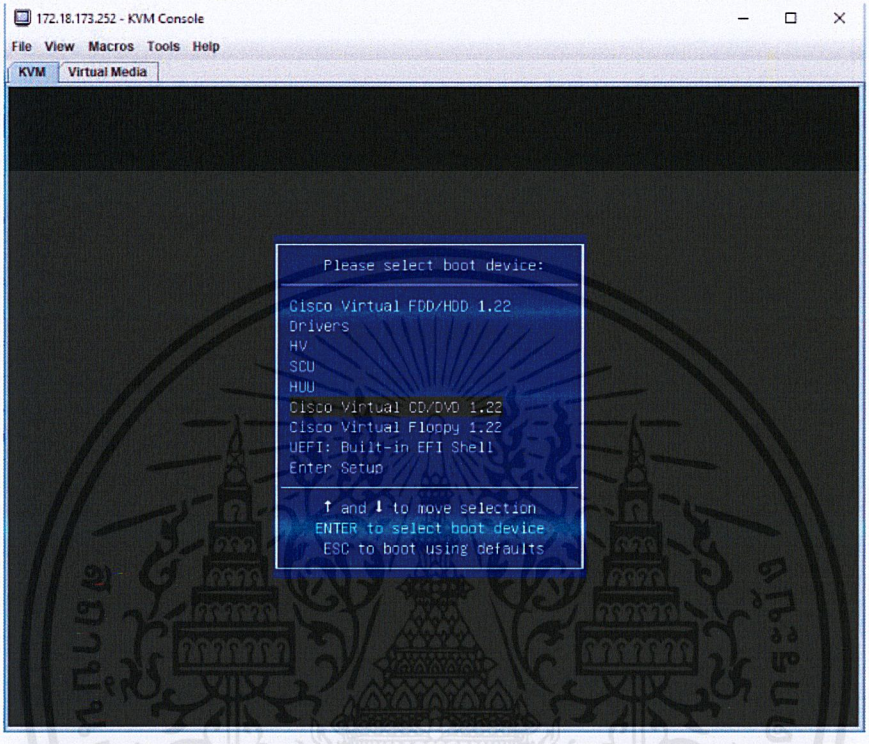


รูปที่ 3.2 หน้าเว็บการจัดการของ CIMC

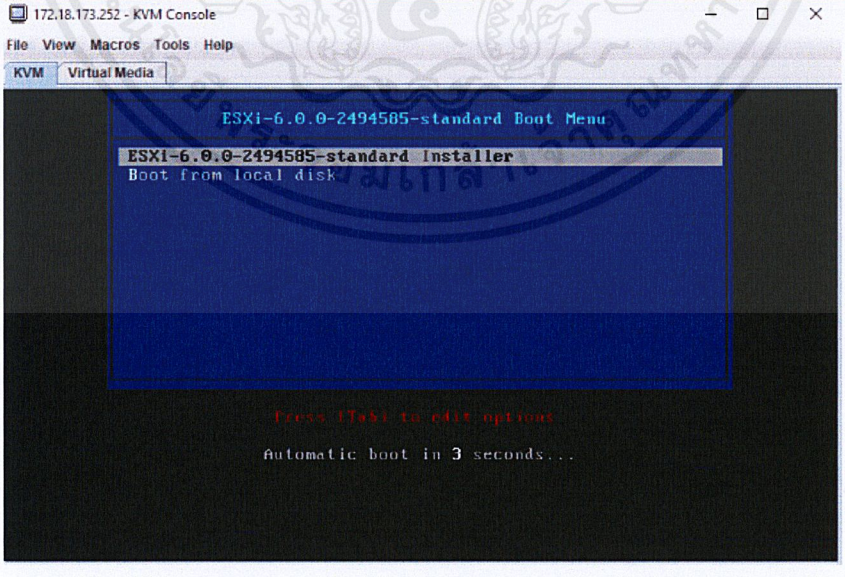
3.3.3. การติดตั้ง VMware ESXi

โดยติดตั้งลงไปยัง Cisco UCS C220 M3 Rack Server เพื่อใช้ในการสร้างและจัดการ Guest OS ที่จะถูกติดตั้งและนำมาใช้ในระบบเครือข่าย โดยต้องมีการนำไฟล์ที่ใช้สำหรับติดตั้งของ VMware ESXi มาอัพโหลดไว้บน Rack Server ก่อน จากนั้นจึงทำการเข้าจัดการผ่านทาง KVM Console เพื่อให้สามารถเลือกBootไฟล์ที่ต้องการติดตั้งได้

- เมื่อเข้าสู่ KVM Consoleแล้ว ให้ทำการกดปุ่ม f6 เพื่อเข้าสู่ Boot Menu แล้วทำการเลือก boot devices ที่ได้อัพโหลดไฟล์สำหรับติดตั้ง VMware ESXi เอาไว้ ในที่นี้ได้ทำการอัพโหลดไปไว้ใน Cisco Virtual CD/DVD 1.22 ดังรูปที่ 3.3 และเลือกไฟล์ติดตั้งตามรูปที่ 3.4

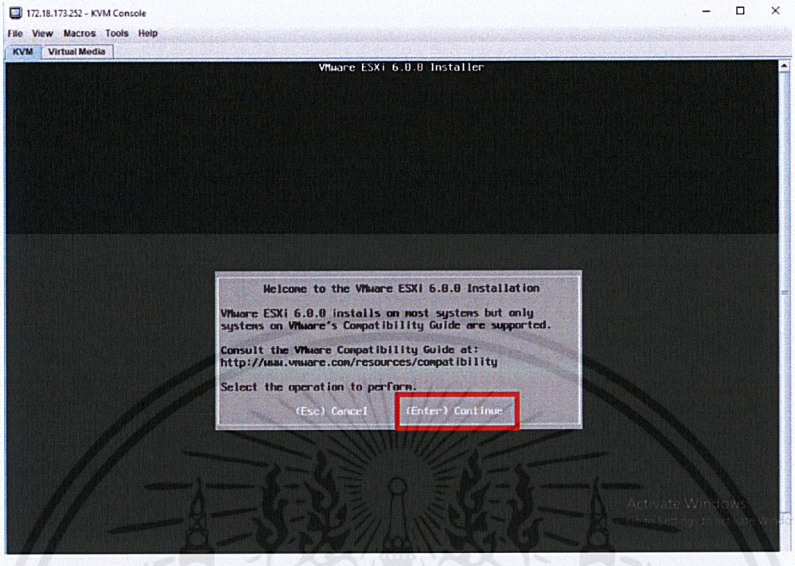


รูปที่ 3.3 การเลือก boot devices



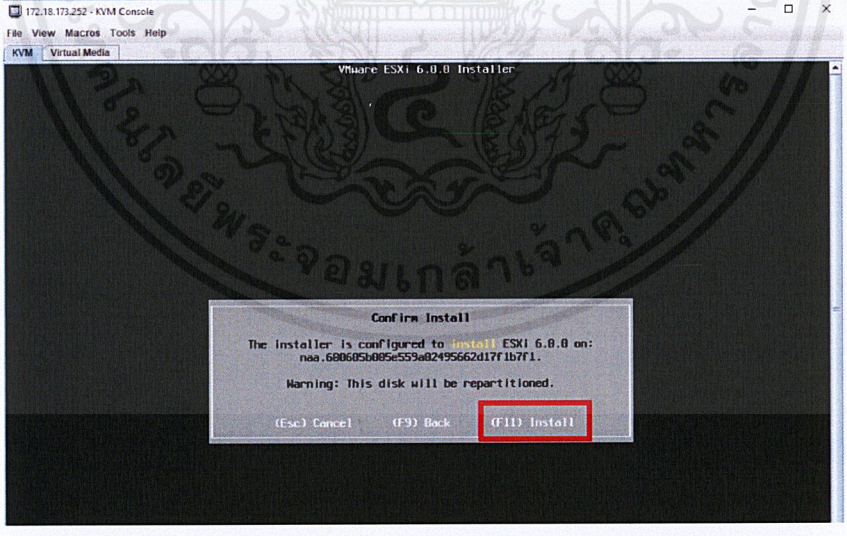
รูปที่ 3.4 การเลือกไฟล์ติดตั้ง VMware ESXi

- เมื่อเลือกไฟล์ที่ต้องการติดตั้งอย่างถูกต้องแล้วก็จะเป็นการเข้าสู่การตั้งค่าพื้นฐาน ซึ่งได้แก่ การเลือก Disk ที่จะทำการติดตั้ง VMware ESXi และการตั้งค่า root password ดังรูปที่ 3.5



รูปที่ 3.6 การเข้าสู่การตั้งค่าพื้นฐาน VMware ESXi

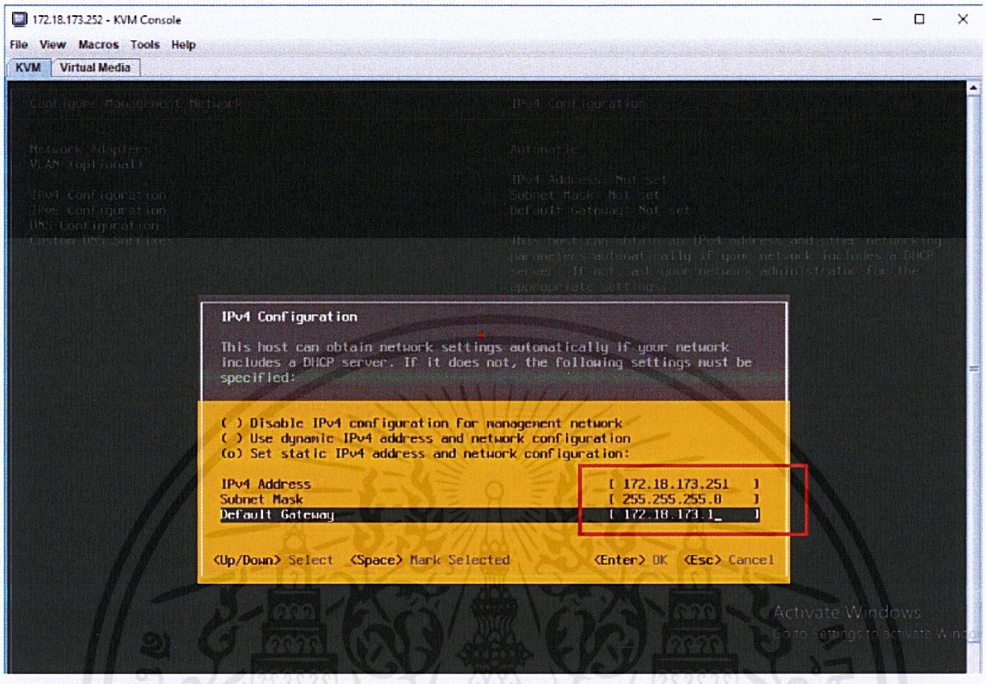
- เมื่อทำการตั้งค่าดังกล่าวเสร็จเรียบร้อยก็จะสามารถเข้าสู่การติดตั้งในขั้นตอนต่อไปได้ ดังรูปที่ 3.7



รูปที่ 3.7 การเข้าสู่การติดตั้ง VMware ESXi

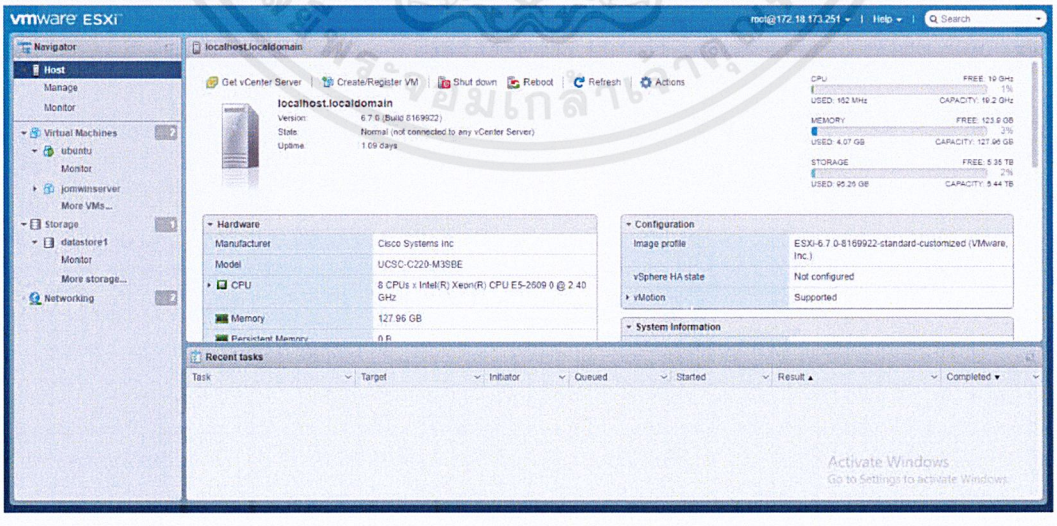
- จากนั้นเมื่อทำการติดตั้งเสร็จจะมีการเข้าไปตั้งค่าเพิ่มเติมให้กับ VMware ESXi ได้แก่ การตั้งค่า IP Address สำหรับการเข้าใช้งาน โดยกำหนดให้มีการตั้งค่า IP Address, Subnet Mask และ

Default Gateway เป็น 172.18.173.251, 255.255.255.0 และ 172.18.173.1 ตามลำดับ ดังรูปที่ 3.8



รูปที่ 3.8 การตั้งค่า IP Address สำหรับการเข้าใช้งาน VMware ESXi

- เมื่อทำการตั้งค่าสร็จเรียบร้อยก็จะสามารถเข้าใช้งาน VMware ESXi ผ่านทาง IP Address 172.18.173.251 และทำการ Login โดยใช้ root password ที่ได้มีการตั้งค่าไว้ในขั้นตอนก่อนหน้า

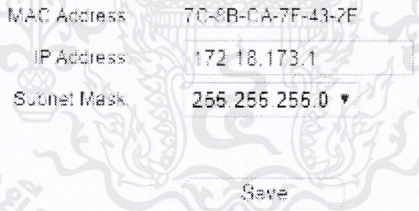


รูปที่ 3.9 หน้าเว็บการจัดการ VMware ESXi

3.3.4. การตั้งค่าให้ Gateway

โดยทำการการตั้งค่า Gateway ที่ใช้เชื่อมต่อกับอินเตอร์เน็ตที่ให้บริการโดย Internet Service Provider จากภายนอก โดยก่อนจะมีการเริ่มใช้งานนั้นจะต้องมีการ Quick Setup ให้แก่อุปกรณ์คือต้องมีการตั้งค่าเบื้องต้นได้แก่

- การตั้งค่า Region ให้ตั้งค่าเป็น (GMT+07.00) Bangkok, Jakarta, Hanoi, Novosibirsk
- การตั้งค่า Dial Up ในที่นี้ไม่จำเป็นต้องแก้ไขหรือปรับแก้เพิ่มเติมใดๆ เนื่องจากต้องการใช้การตั้งค่าดั้งเดิมของซิมการ์ดที่ได้รับมาจาก Internet Service Provider ภายนอก
- การตั้งค่า Wireless Radio ซึ่งในที่นี้ยังไม่มีความจำเป็นที่ต้องใช้งาน จึงสามารถ Disable ไว้ก่อนแล้วข้ามขั้นตอนนี้ไปได้
- เมื่อเสร็จสิ้นการ Quick Setup แล้ว ก็ให้ทำการตั้งค่า LAN ใหม่ จาก IP Address เดิมคือ 192.168.1.1 เป็น 172.18.173.1 ดังรูปที่ 3.9 เพื่อทำให้อุปกรณ์ตัวนี้ทำหน้าที่เสมือนกับเป็น Gateway สำหรับใช้งานอินเทอร์เน็ต

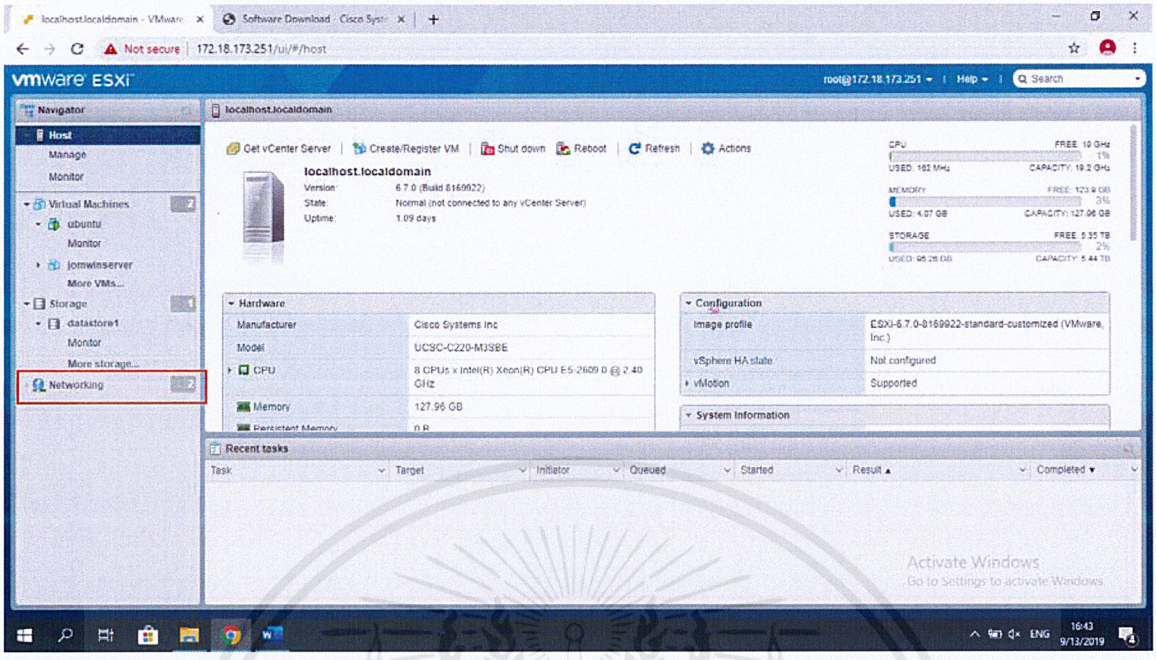


รูปที่ 3.9 การตั้งค่า LAN

3.3.5. การสร้าง Network Adapter ภายใน VMware ESXi

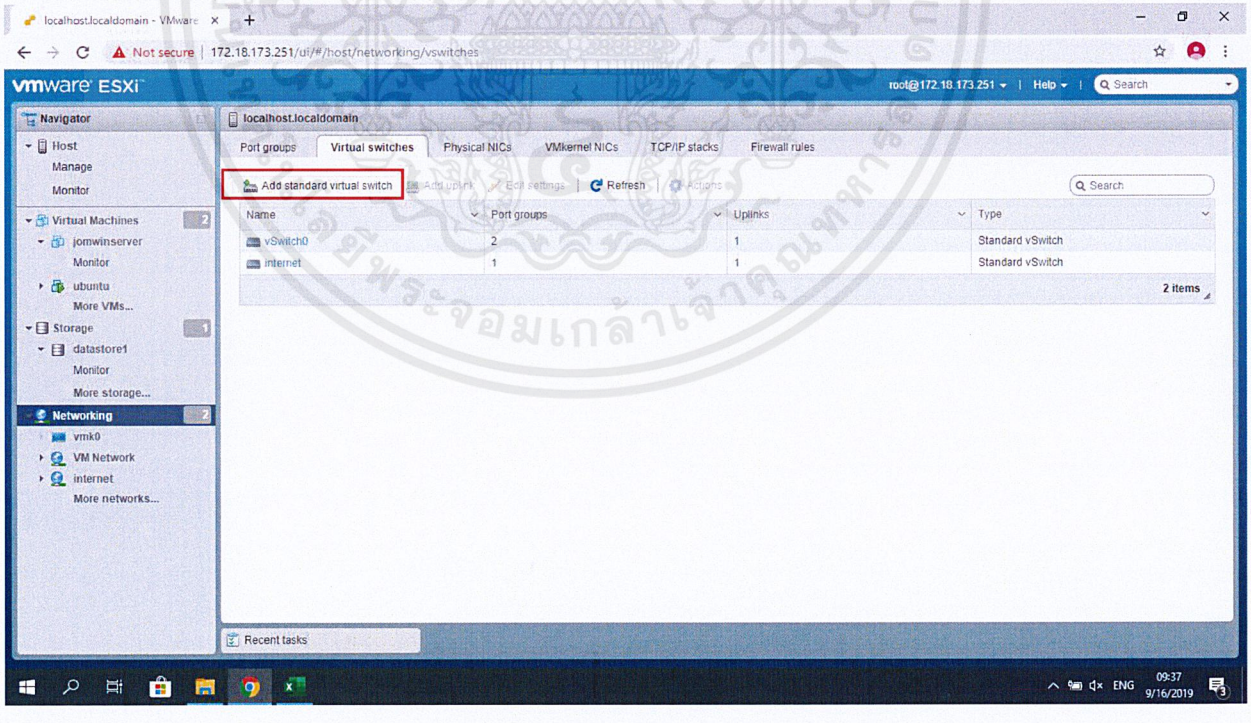
สำหรับให้ Guest OS ที่จะถูกสร้างขึ้นในอนาคตใช้เพื่อเชื่อมต่อกับอินเทอร์เน็ต

- โดยทำการเข้าสู่หน้าหลักของ VMware ESXi แล้วทำการเลือกเมนู Networking ที่แถบด้านซ้าย ดังรูปที่ 3.10

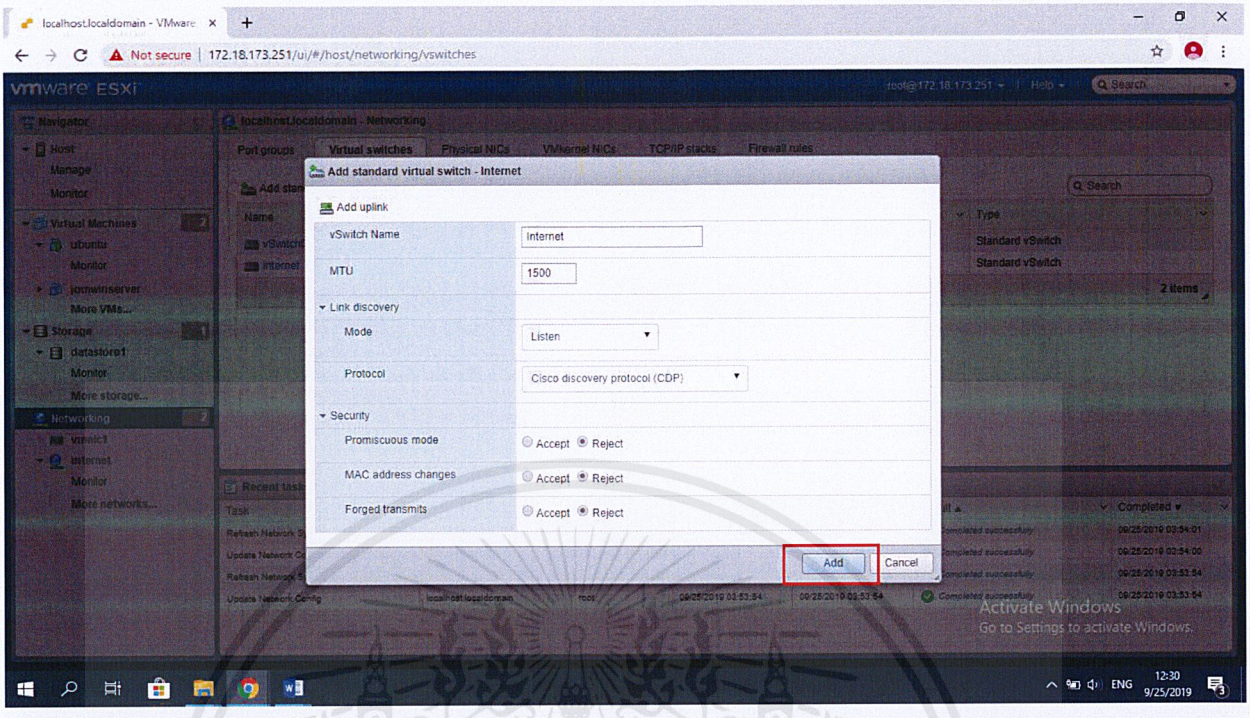


รูปที่ 3.10 การเลือกเมนู Networking

- จากนั้นทำการ Add Standard Virtual Switch ขึ้นมาใหม่ โดยตั้งชื่อว่า internet ดังรูปที่ 3.11 และ 3.12

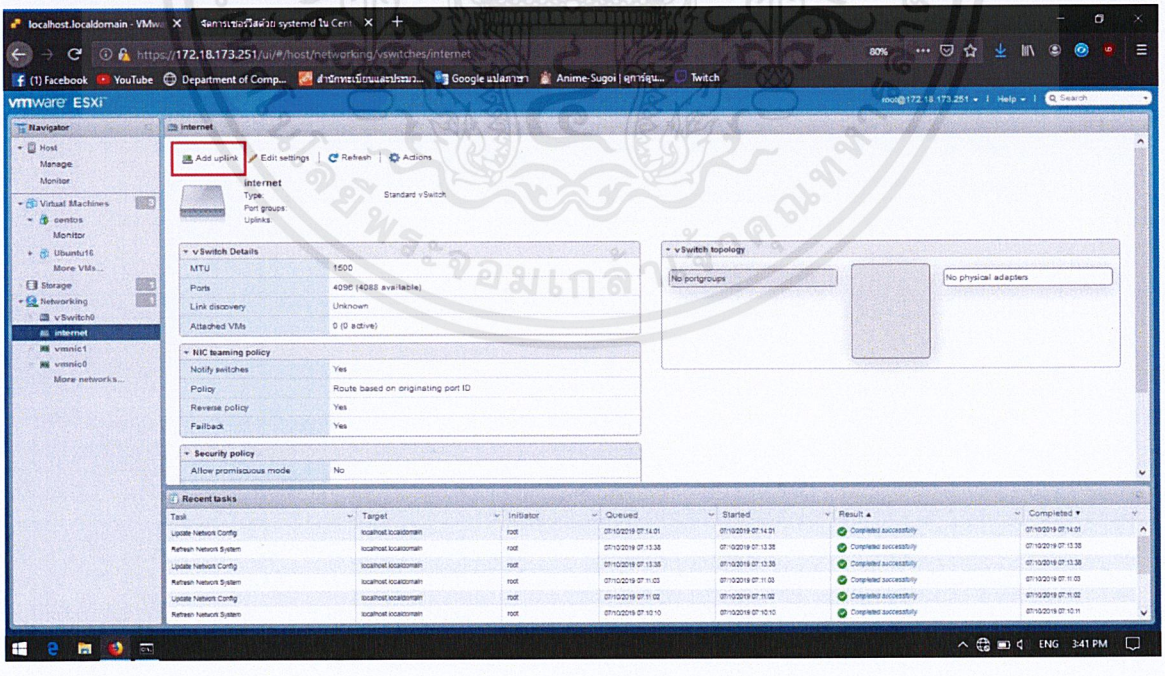


รูปที่ 3.11 การเพิ่ม Standard virtual switch 1

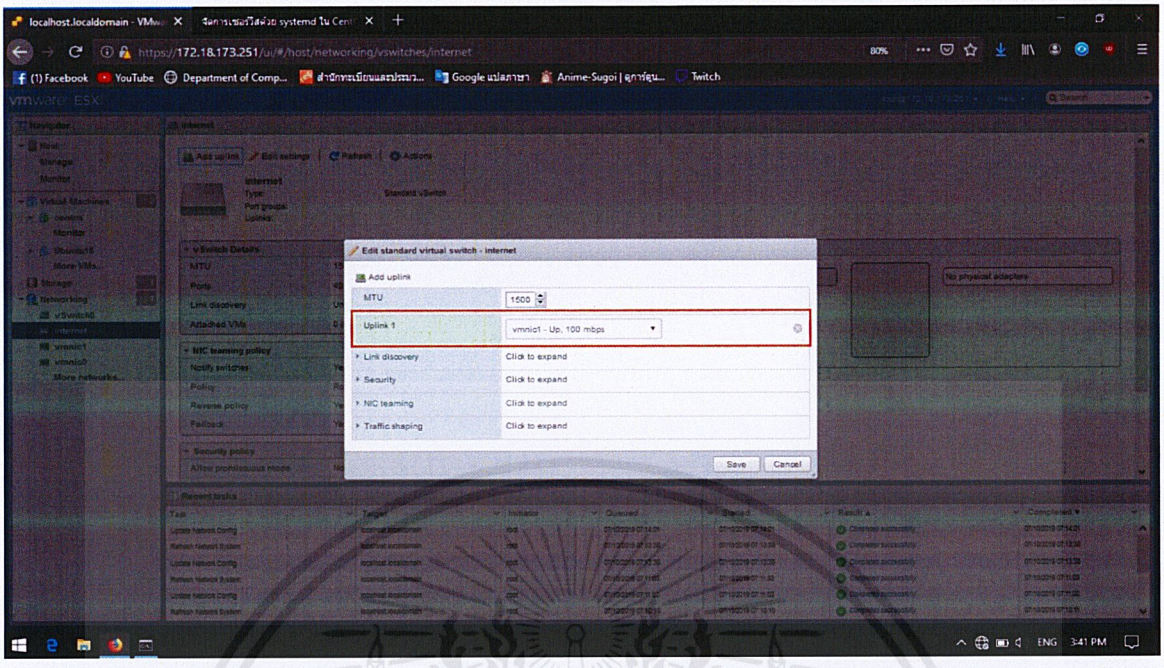


รูปที่ 3.12 การเพิ่ม Standard virtual switch 2

- จากนั้นทำการเข้าไปเพิ่ม Uplink ให้กับ Virtual Switch โดยทำการเพิ่ม vmnic1 ซึ่งเป็น Uplink ของ TP-Link ที่สามารถใช้ในการเข้าถึงอินเทอร์เน็ตได้

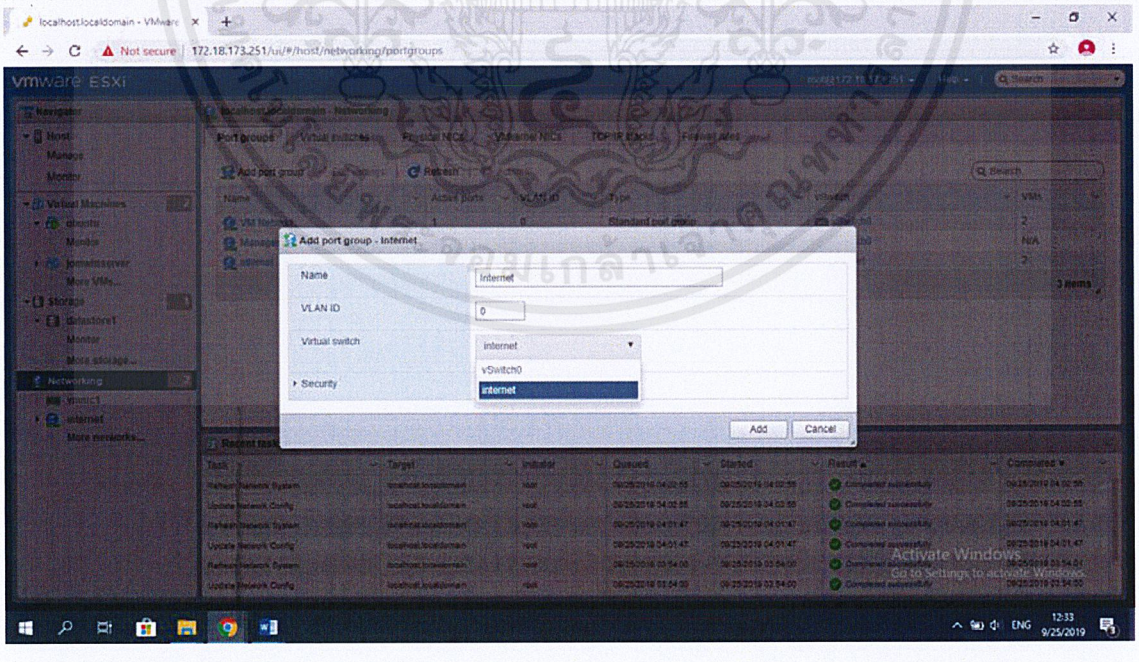


รูปที่ 3.13 การเพิ่ม Uplink ให้กับ Virtual Switch 1



รูปที่ 3.14 การเพิ่ม Uplink ให้กับ Virtual Switch 2

- จากนั้นเมื่อทำการเพิ่ม Uplink เสร็จเรียบร้อย ก็ทำการสร้าง Port Group ขึ้นมาใหม่โดยใช้ชื่อว่า internet แล้วทำการจับคู่ Port Group นี้เข้ากับ Virtual Switch ที่สร้างไว้ก็คือ internet ดังรูปที่ 3.15

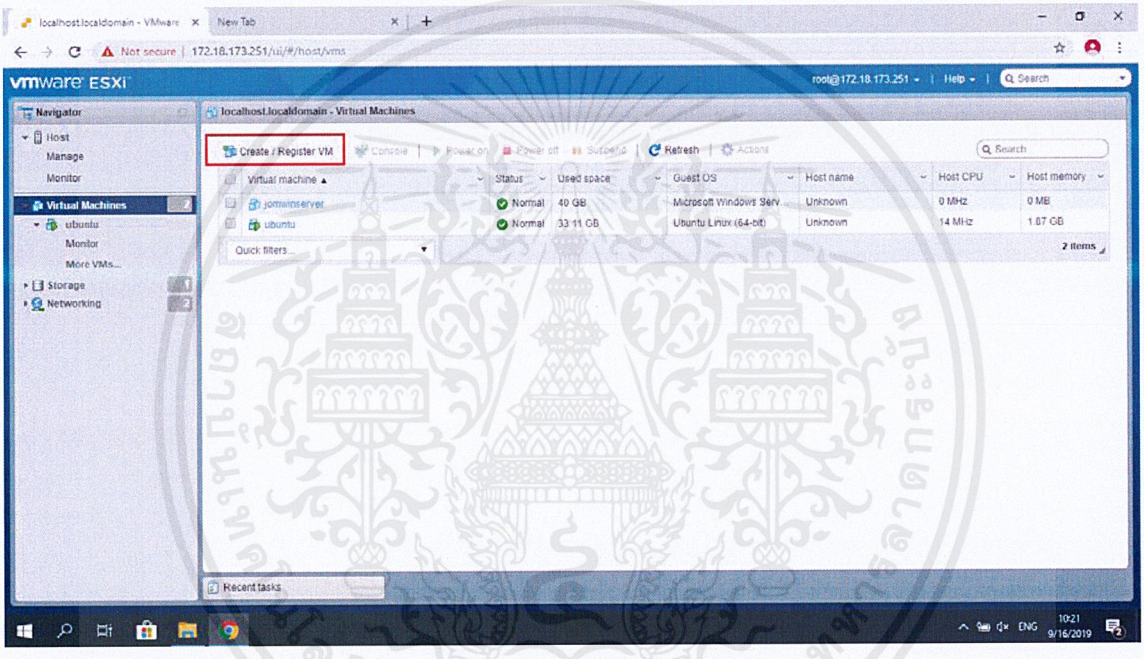


รูปที่ 3.15 การสร้าง Port Group และเพิ่ม Virtual Switch ให้ Port Group

3.3.6. การสร้าง Guest OS ตัวที่ 1

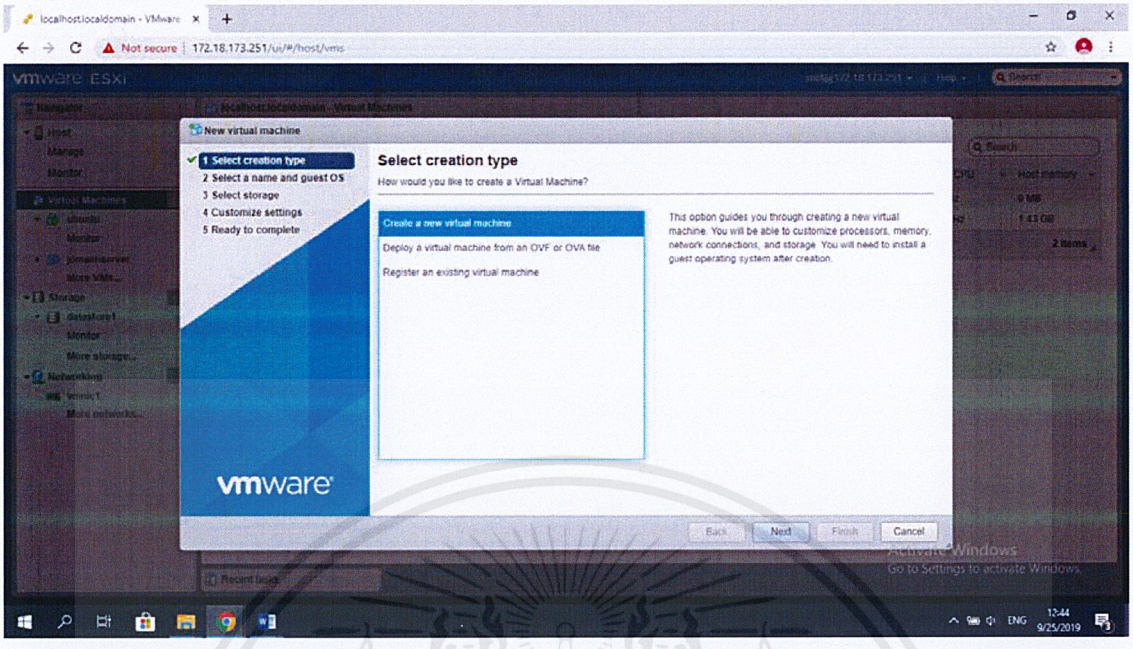
ใช้ระบบปฏิบัติการ Ubuntu 18.04 โดยก่อนจะทำการสร้าง Guest OS ที่ต้องการนั้นก็ต้องทำการอัพโหลดไฟล์สำหรับติดตั้งระบบปฏิบัติการเข้าไปใน datastore1 ซึ่งเป็น storageที่ใช้เก็บข้อมูลของ VMware ESXi ก่อน

- จากนั้นก็ทำการสร้าง Virtual Machine โดยเข้าสู่หน้าหลักของ VMware ESXi แล้วเลือกเมนู Virtual Machines ที่แถบด้านซ้ายมือ จากนั้นทำการ Create/Register VM ดังรูปที่ 3.16



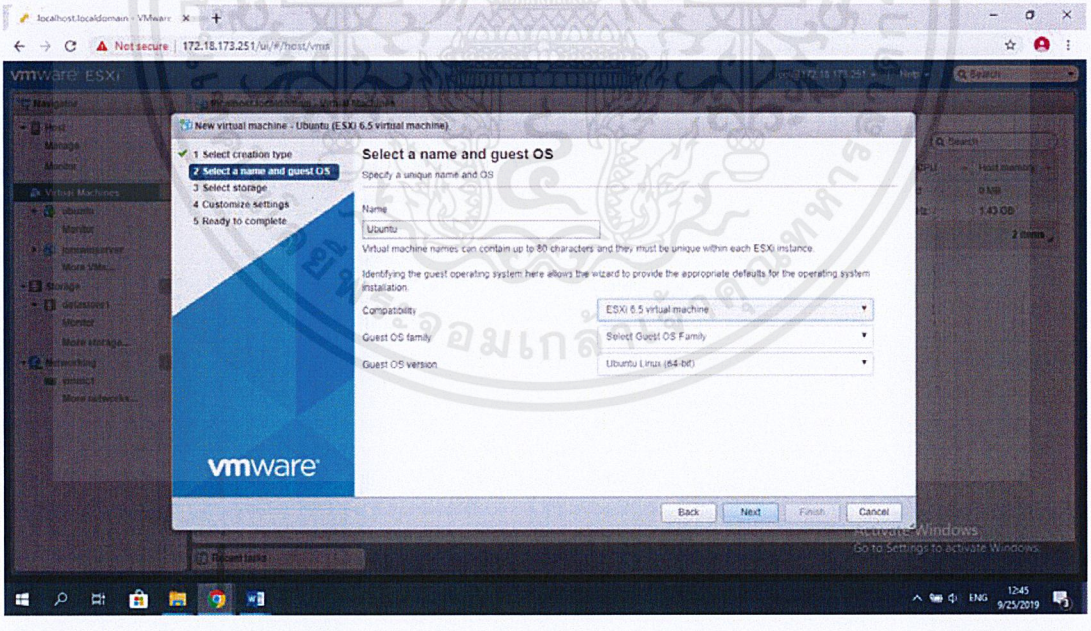
รูปที่ 3.16 การเลือกสร้าง VM

- เมื่อกด Create/Register VM จะเข้าสู่หน้าต่างการสร้าง Virtual Machine แล้วก็ให้ทำการเลือกไปที่ Create a new virtual machine ดังรูปที่ 3.17



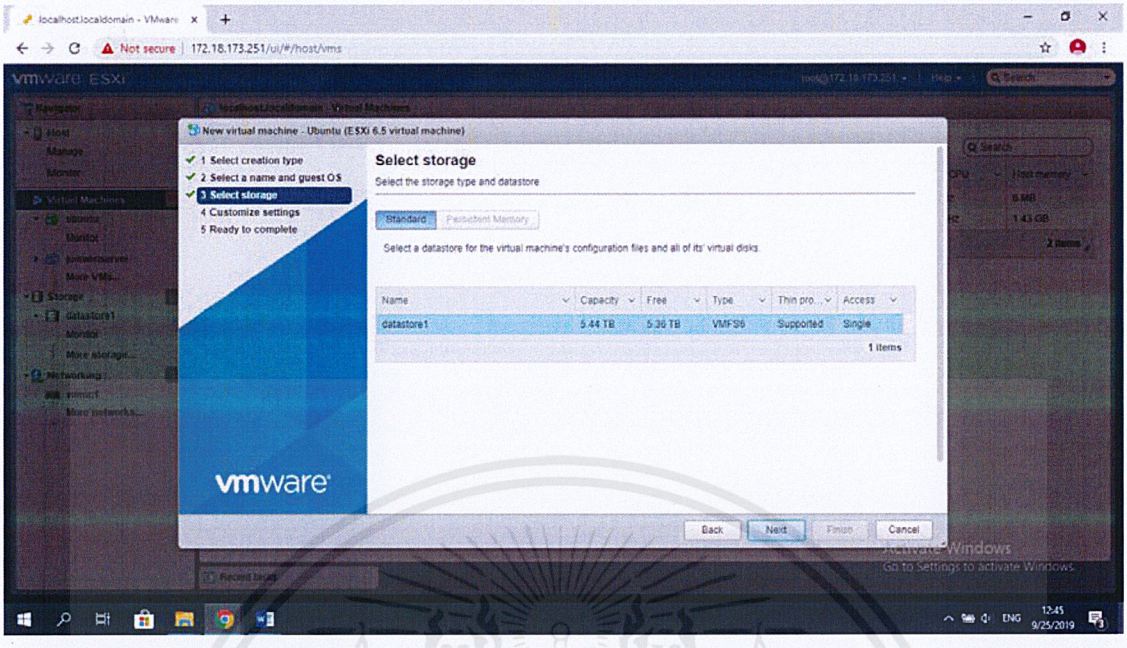
รูปที่ 3.17 การสร้าง VM ขึ้นใหม่

- ทำการตั้งชื่อและเลือกระบบปฏิบัติการที่จะใช้สำหรับ Guest OS ตัวนี้ โดยในที่นี้จะใช้เป็น Ubuntu Linux (64-bit)



รูปที่ 3.18 การตั้งชื่อและเลือกระบบปฏิบัติการให้กับ VM

- ทำการเลือก storage ที่จะใช้เก็บข้อมูล โดยเลือก datastore1 ซึ่งเป็นฐานข้อมูลที่ถูกสร้างขึ้นมาพร้อมกับการติดตั้ง VMware ESXi



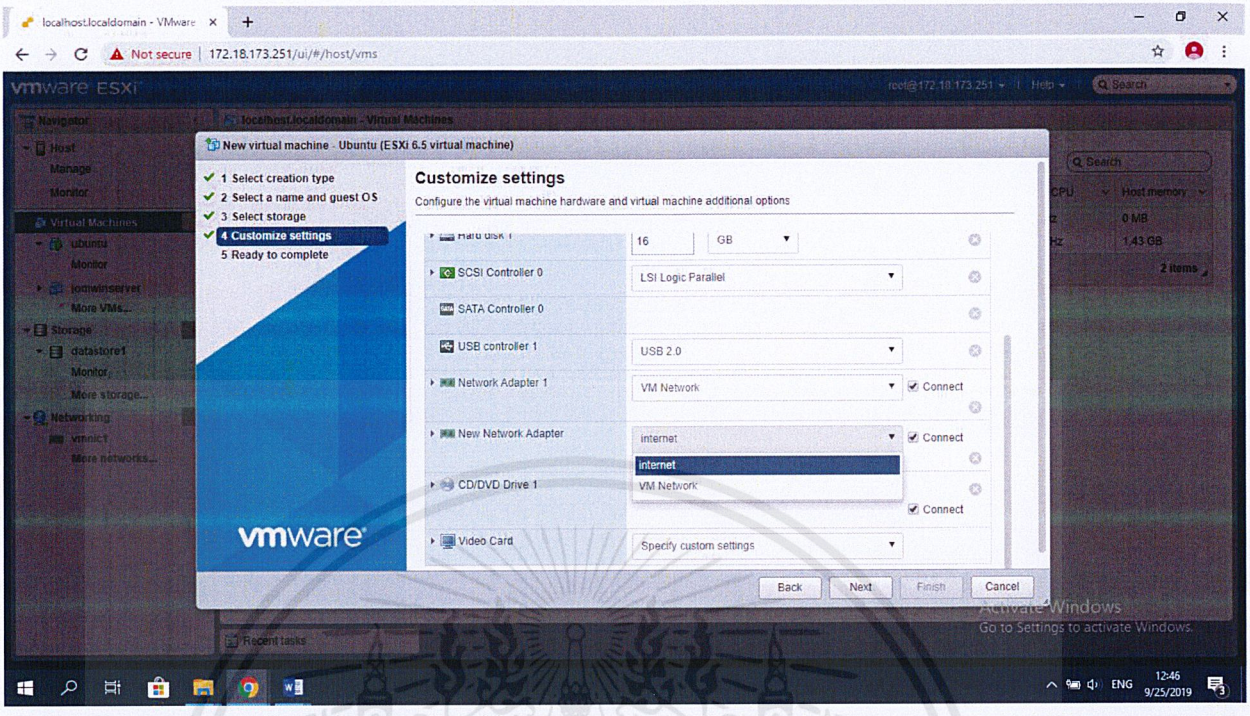
รูปที่ 3.19 การเลือก Storage สำหรับการเก็บข้อมูล

- จากนั้นจะเป็นการตั้งค่า Hardware Settings ซึ่งสามารถกำหนด Spec ของเครื่อง Guest OS ตัวนี้ได้ตามความเหมาะสมในการใช้งาน โดยกำหนดการตั้งค่าตามตารางที่ 3.4

ตารางที่ 3.4 Hardware Settings ของ Guest OS ตัวที่ 1

CPU	2 CPUs
Memory	8 GB
Harddisk	25 GB
Network Adapter 1	VM Network
Network Adapter 2	internet
CD/DVD Drive	Datastore1/ubuntu-18.04.2-desktop.iso

- ในที่นี้ต้องทำการ Add network adapter เพิ่มขึ้นมาจากเดิมอีก1ตัวเพื่อให้ Guest OS ใช้สำหรับเข้าถึงอินเทอร์เน็ตได้ โดยให้เลือกใช้งาน Port Group internet ที่สร้างไว้ ดังรูปที่ 3.20 (Network Adapter ตัวที่1จะทำหน้าที่ในเชื่อมต่อ Guest OS ทั้งหมดให้สามารถติดต่อกับ Hostและติดต่อกันเองภายใน Host ได้)



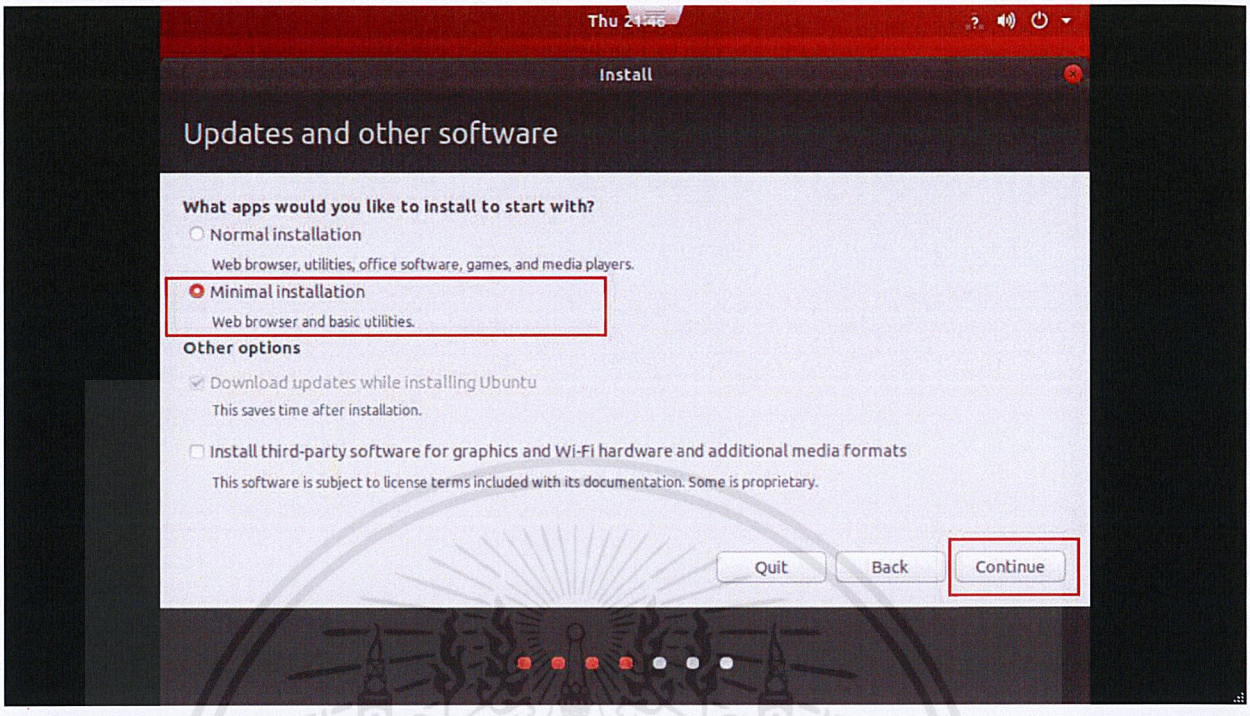
รูปที่ 3.20 การเพิ่ม Network Adapter ให้กับ VM

- เมื่อสร้าง Guest OS เสร็จสิ้นก็ทำการเปิดการทำงานขึ้นมาโดยกดปุ่ม Power on เพื่อทำการเข้าสู่การติดตั้งในขั้นตอนต่อไป

3.3.7. การติดตั้ง Ubuntu Desktop 18.04

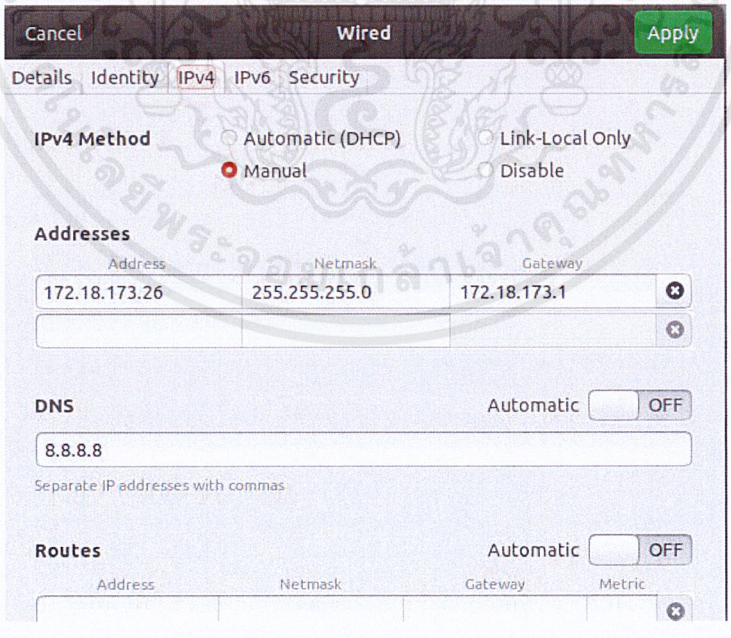
เมื่อเปิดการทำงานของ Virtual Machine ที่สร้างไว้ ก็จะเป็นการเข้าสู่การติดตั้งระบบปฏิบัติการตามที่ได้เลือกไว้

- ทำการติดตั้งแบบ Minimal Installation ดังรูปที่ 3.21 เพื่อเป็นการลดสิ่งที่ไม่จำเป็นในการใช้งานออกไป แล้วให้ทำการติดตั้งต่อไปตามขั้นตอน โดยกำหนด Hostname ให้กับ Ubuntu เครื่องนี้ว่า server01



รูปที่ 3.21 การเลือกติดตั้ง Ubuntu 18.04 แบบ Minimal installation

- เมื่อทำการติดตั้งเสร็จก็ทำการเข้าสู่หน้า Desktop เพื่อเข้าไปตั้งค่า IP Address และ Default Gateway ให้เป็น 172.18.173.26 และ 172.18.173.1 ดังรูปที่ 3.22



รูปที่ 3.22 การตั้ง IP Address ให้กับ server01

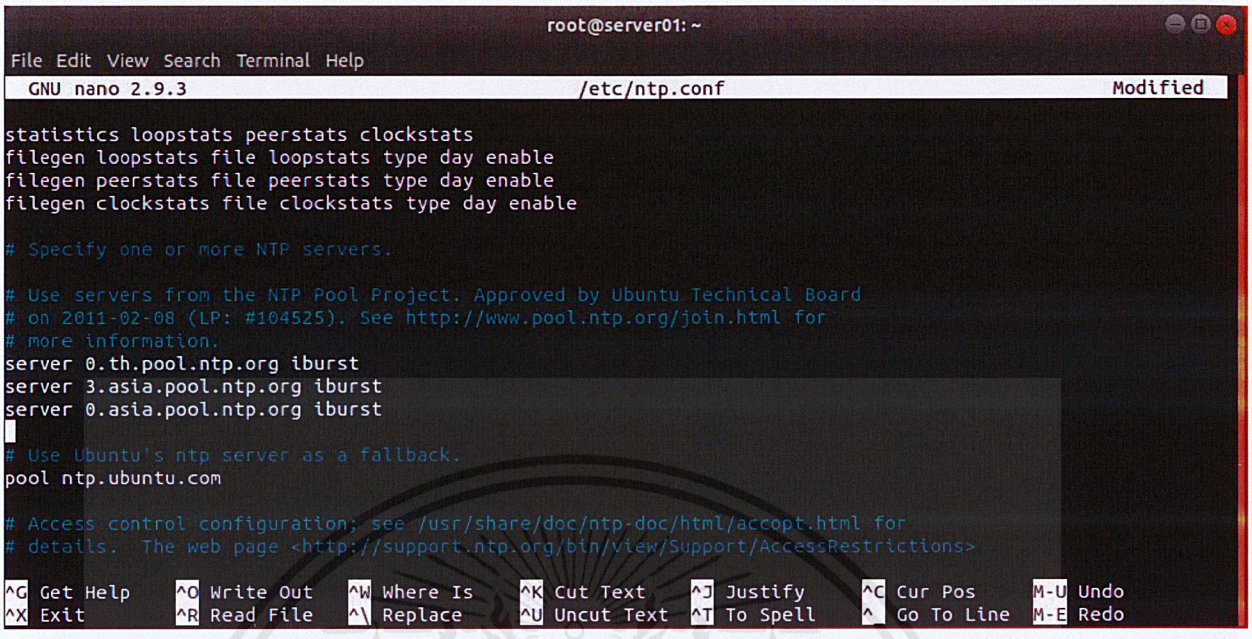
3.3.8. การติดตั้งส่วนประกอบเพิ่มเติมลงบน Ubuntu 18.04 server

โดยทำการติดตั้งส่วนประกอบเพิ่มเติม ได้แก่ NTP Server, Radius Server, DHCP Server และ OpenSSH Server เพื่อให้ Guest OS ตัวนี้ทำหน้าที่เป็น Authentication Server สำหรับจำกัดการเข้าจัดการอุปกรณ์ในระบบเครือข่ายและจำกัดการเข้าถึงเครือข่ายภายในองค์กร

- อันดับแรกต้องทำการอัพเดทเวอร์ชั่นของระบบปฏิบัติการโดยเข้าสู่หน้า Console และใช้คำสั่ง apt-get update
- ติดตั้ง NTP Server โดยใช้คำสั่ง apt-get install ntp
- ทำการตรวจสอบการทำงานของ NTP Server โดยใช้คำสั่ง service ntp status ดังรูปที่ 3.23

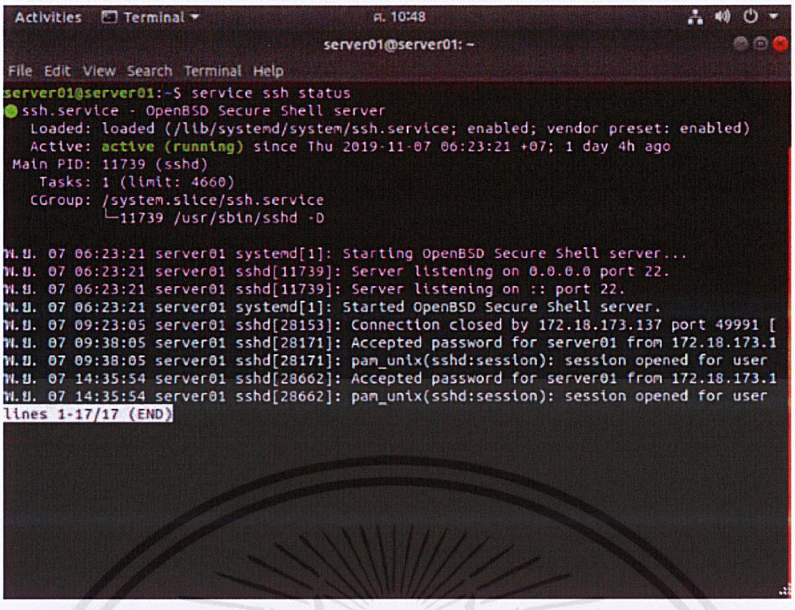
รูปที่ 3.23 การแสดงผลสถานะการทำงานของ NTP Server

- ทำการเข้าไปตั้งค่า NTP Pool ภายในไฟล์ ntp.conf ให้ชี้ไปยังServerที่ใกล้ที่สุด คือ ประเทศไทย ดังรูปที่ 3.24 ใช้คำสั่งคือ sudo nano /etc/ntp.conf โดยสามารถเข้าไปค้นหาNTP Serverได้จาก https://www.pool.ntp.org/zone/th



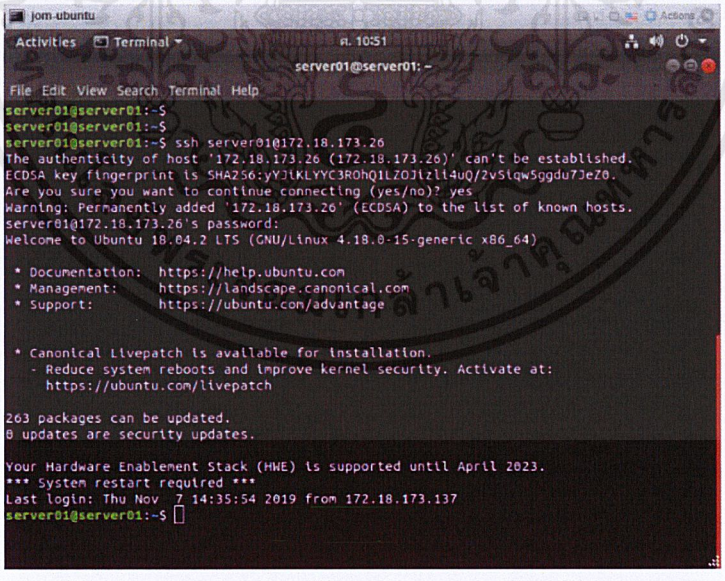
รูปที่ 3.24 การตั้งค่า NTP Pool ภายในไฟล์ ntp.conf

- แล้วจากนั้นทำการ Restart NTP โดยใช้คำสั่ง service ntp restart
- เมื่อเสร็จสิ้นการตั้งค่าก็ให้ทำการแก้ไข Rules เพื่อให้ Client อื่นๆภายในระบบสามารถนำ NTP Server ไปใช้งานได้ โดยใช้คำสั่ง sudo ufw allow from any to any port 123 proto udp
- ติดตั้ง OpenSSH Server เพื่อให้เข้าจัดการหน้า Console ของ Ubuntu 18.04 ได้สะดวกมากขึ้น โดยใช้คำสั่ง apt-get install openssh-server โดยเมื่อติดตั้งเสร็จสามารถตรวจสอบการทำงานโดยใช้คำสั่ง service ssh status ดังรูปที่ 3.25



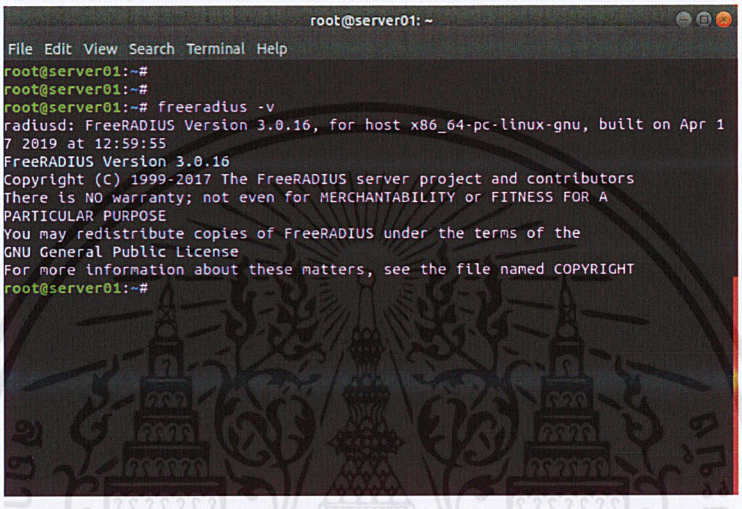
รูปที่ 3.25 การแสดงผลสถานะการทำงานของ OpenSSH Server

- ทำการสร้างการเชื่อมต่อเพื่อให้สามารถเข้าใช้งาน Ubuntu ตัวนี้ที่มี hostname คือ server01 ผ่านทางโปรโตคอล SecureShell(SSH) ด้วย IP 172.18.173.26 โดยการใช้คำสั่ง ssh server01@172.18.173.26 ดังรูปที่ 3.26



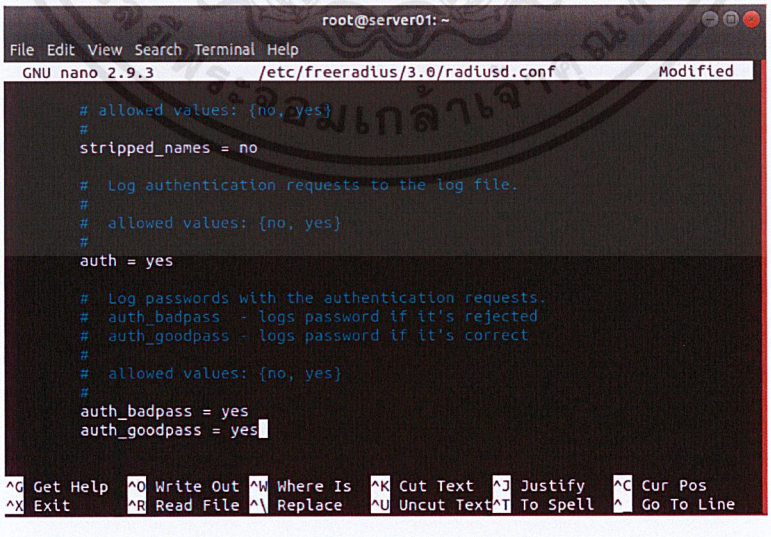
รูปที่ 3.26 การสร้างการเชื่อมต่อเข้ามายัง server01 ผ่านโปรโตคอล SSH

- เมื่อผลการเชื่อมต่อเป็นไปดังรูปที่ 3.26 ก็ให้ทำการป้อนคำสั่ง logout เป็นอันเสร็จสิ้นการติดตั้ง OpenSSH Server และในส่วนของการทดสอบการเข้าใช้งานผ่านโปรแกรม putty จะขอกล่าวถึงในบทที่ 4
- ติดตั้ง FreeRADIUS โดยใช้คำสั่ง apt-get install freeradius พร้อมทั้งตรวจสอบเวอร์ชั่นของโปรแกรมFreeRADIUS โดยใช้คำสั่ง freeradius -v ดังรูปที่ 3.27



รูปที่ 3.27 การตรวจสอบเวอร์ชั่นของ FreeRADIUS ที่ทำการติดตั้งไป

- ทำการตั้งค่าโปรแกรม FreeRADIUS ให้มีการแสดงผลlog โดยใช้คำสั่ง sudo nano /etc/freeradius/3.0/radiusd.conf เข้าไปแก้ไขการตั้งค่าในไฟล์ radiusd.conf ดังรูปที่ 3.28

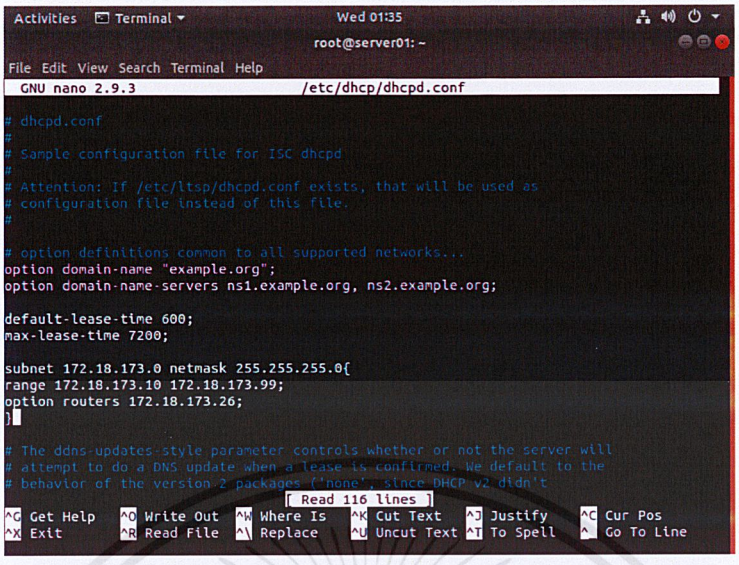


รูปที่ 3.28 การตั้งค่าภายในไฟล์ radiusd.conf

- ทำการเข้าเพิ่ม clients (ในที่นี้คืออุปกรณ์ในระบบเครือข่าย) เข้าไปใน FreeRADIUS โดยทำการเพิ่มอุปกรณ์ได้แก่ Management Switch, Access Switch, Wireless LAN Controller(WLC) และ Cisco Access Point ตาม IP Address ในตารางที่ 3.3

รูปที่ 3.29 การเพิ่ม Clients ให้กับ FreeRADIUS

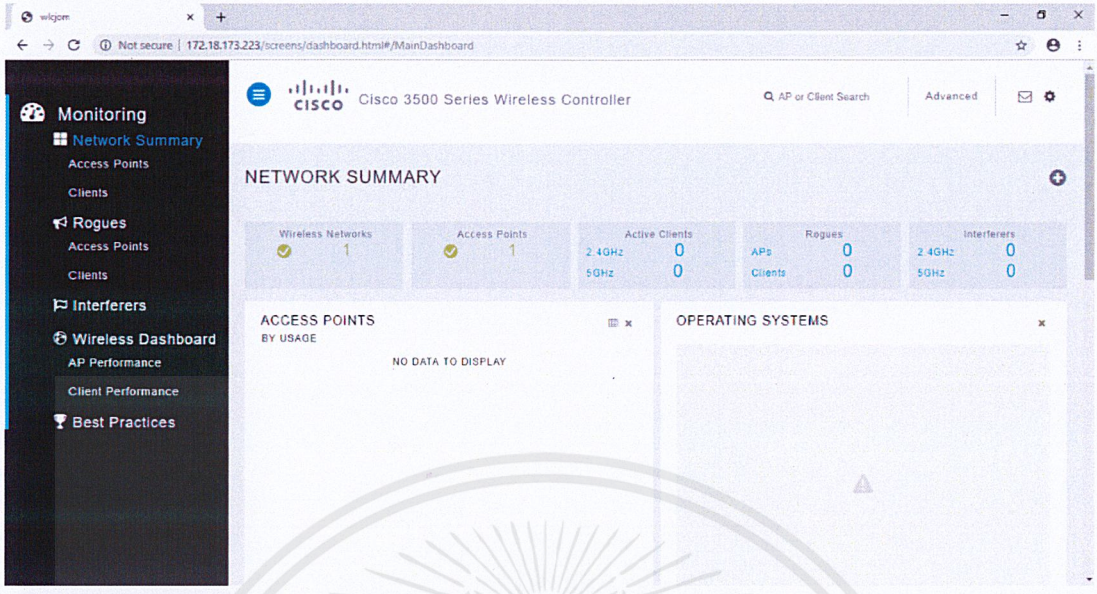
- ทำการสร้างบัญชี User สำหรับเข้าถึงเครือข่ายภายในขององค์กร และบัญชี User ที่มีสิทธิ์เข้าถึงการจัดการอุปกรณ์ต่าง ๆ ในระบบเครือข่ายได้ โดยทำการสร้างไว้ภายใน /etc/freeradius/3.0/users
- ทำการติดตั้ง DHCP Server โดยใช้คำสั่ง apt-get install isc-dhcp-server และทำการเข้าปรับแก้การแจกIP Address ของ DHCP Server ในไฟล์ dhcpd.conf โดยใช้คำสั่ง sudo nano /etc/dhcp/dhcpd.conf ดังรูปที่ 3.30



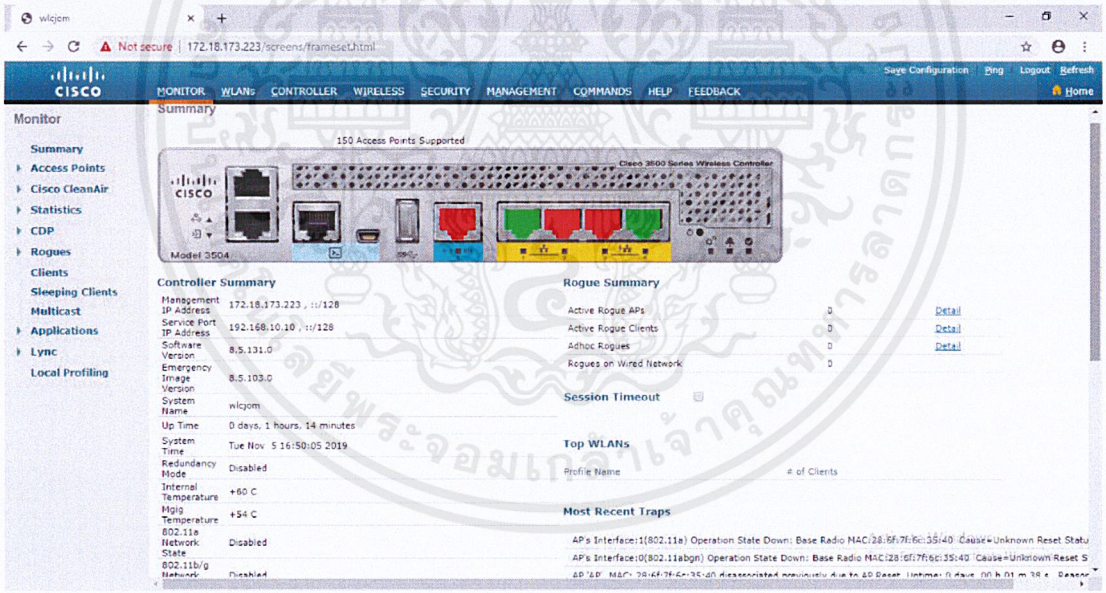
รูปที่ 3.30 การตั้งค่าการทำงานของ DHCP server

3.3.9. การติดตั้ง Wireless LAN Controller (WLC) และ Cisco Access Point

- การ Initial setup คือเมื่อมีการนำ Wireless LAN Controller มาติดตั้งในระบบก็ต้องมีการตั้งค่าเบื้องต้นให้กับอุปกรณ์ก่อนจึงจะสามารถใช้งานได้ โดยในที่นี้จะกำหนดการตั้งค่าเบื้องต้นที่จำเป็น ได้แก่
    1. ตั้งค่า username และ password ที่ใช้ในการเข้าจัดการ Wireless LAN Controller
    2. System Name กำหนดเป็น wlcjom
    3. Management IP Address กำหนดเป็น 172.18.173.223
    4. ทำการสร้าง WLANs ขึ้นมา โดยกำหนดเป็น
    5. จากนั้นจะสามารถเข้าจัดการ Wireless LAN Controller ผ่านทางManagement IP Address ได้
- โดยหน้าเว็บสำหรับการจัดการจะมีหน้าตาดังรูปที่ 3.31 และ 3.32

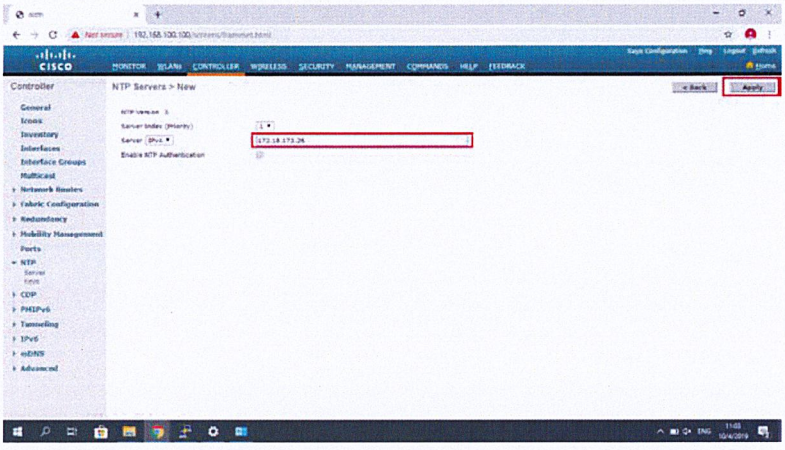


รูปที่ 3.31 หน้าเว็บการจัดการของ WLC 1



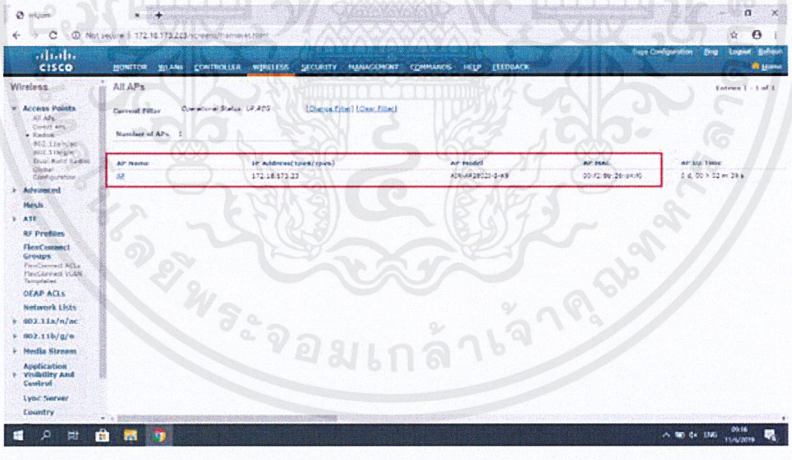
รูปที่ 3.32 หน้าเว็บการจัดการของ WLC 2

- ทำการเพิ่ม NTP Server ให้กับ Wireless LAN Controller เพื่อให้ชี้ไปยัง Ubuntu 18.04 โดยเลือกที่แท็บController -> NTP Servers -> Add new โดยทำการเพิ่ม NTP Server ดังรูปที่ 3.33



รูปที่ 3.33 การเพิ่ม NTP Server บน WLC

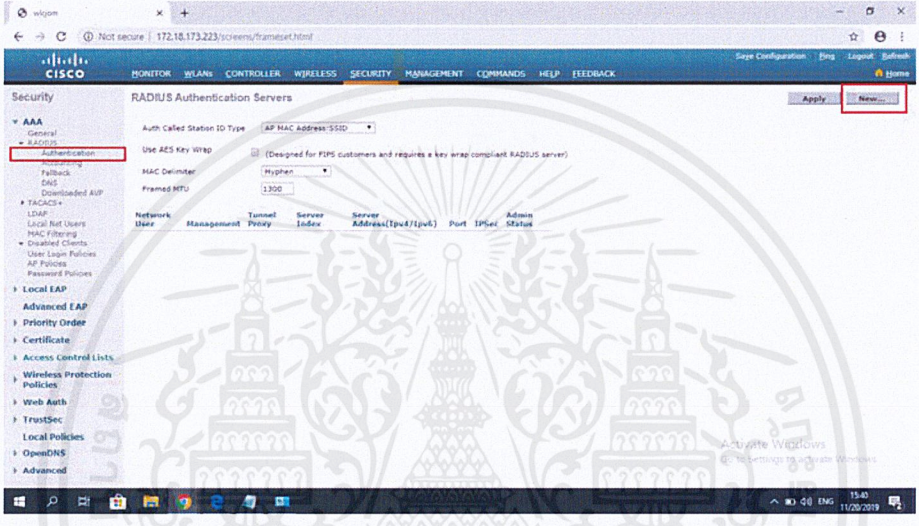
- ตั้งค่า Cisco Access Point โดยการใช้คำสั่งคือ capwap ap primary-base wlcjom 172.18.173.223 ซึ่งเป็นคำสั่งที่ใช้ในการระบุตัว Wireless LAN Controller ที่ต้องการให้ Access Point เชื่อมต่อด้วย โดยในที่นี้จะกำหนดให้มีการเชื่อมต่อไปยัง wlcjom ที่มีIP Address เป็น 172.18.173.223 และเมื่อมีการตั้งค่าให้ AP เชื่อมต่อกับ WLC ที่ติดตั้งไว้เรียบร้อยแล้ว จะสามารถเข้าไปจัดการ AP ที่เชื่อมต่อเข้ามาได้ผ่านทางหน้าเว็บของ WLC ดังรูปที่ 3.34



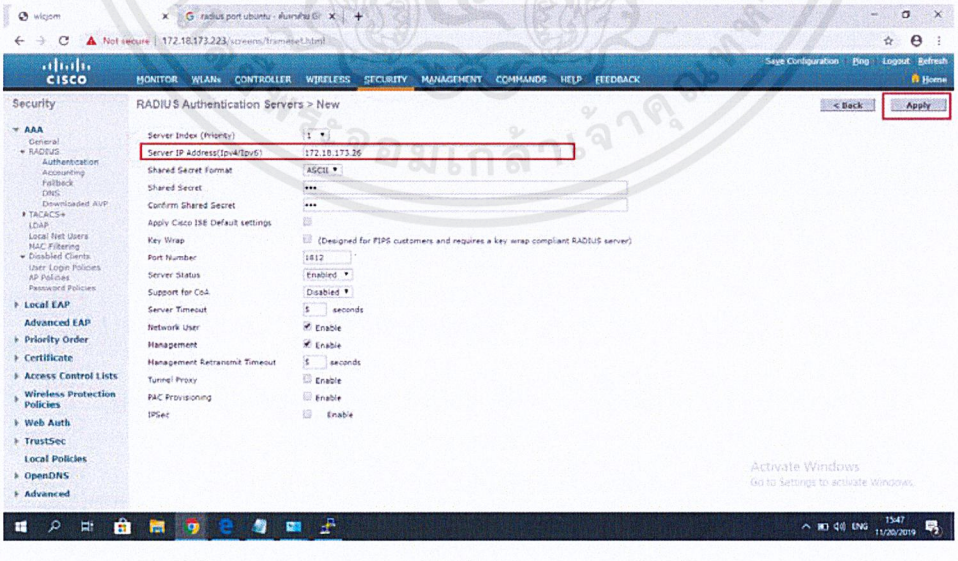
รูปที่ 3.34 หน้าการจัดการ AP ที่มีการเชื่อมต่อเข้ามา

3.3.10. การตั้งค่าระบบยืนยันตัวตนผู้เข้าใช้งานระบบเครือข่ายภายในองค์กร

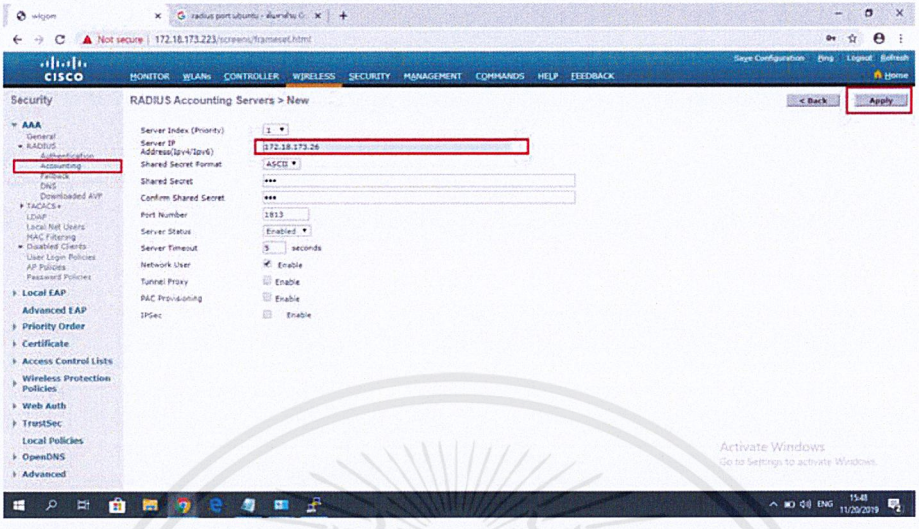
- โดยตั้งค่าให้ WLC ให้ชี้ไปยัง RADIUS Server ที่มีการติดตั้งไว้ใน Ubuntu 18.04 สำหรับให้Userที่จะเข้าใช้งานระบบเครือข่ายได้เข้าไปยืนยันตัวตนกับ RADIUS Server ก่อน โดยเลือกแท็บ Security -> AAA -> RADIUS แล้วจึงทำการเพิ่ม RADIUS Authentication และ Accounting Server ดังรูปที่ 3.35, 3.36 และ 3.37



รูปที่ 3.35 การเพิ่ม RADIUS Authentication Server ภายใน WLC 1



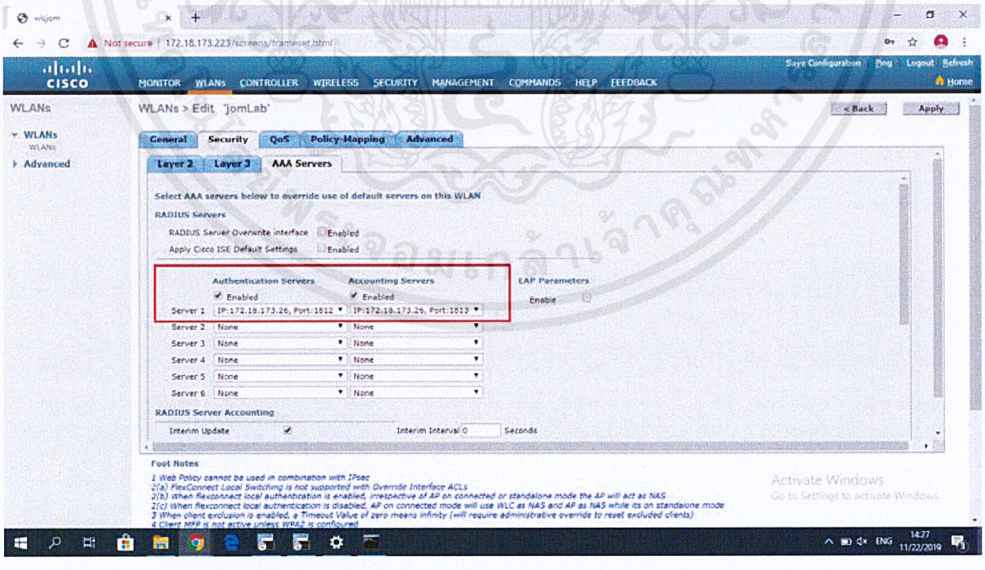
รูปที่ 3.36 การเพิ่ม RADIUS Authentication Server ภายใน WLC 2



รูปที่ 3.37 การเพิ่ม RADIUS Accounting Server ภายใน WLC

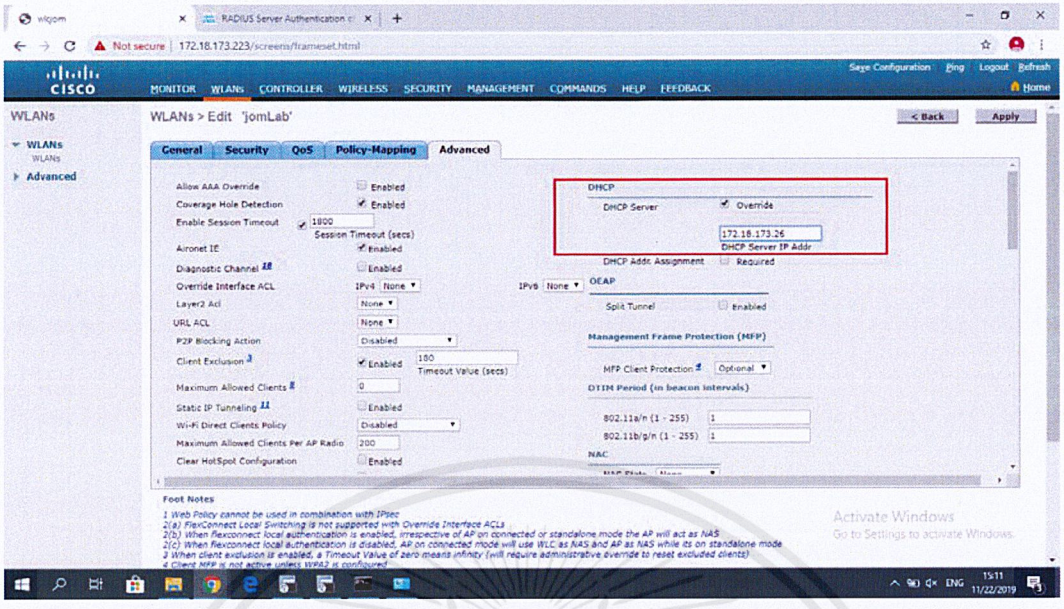
3.3.11. การกำหนดค่าให้ WLANs ได้มีการเรียกใช้การยืนยันตัวตนกับ RADIUS Server

- โดยเข้าไปตั้งค่าภายใน WLANs ที่ต้องการแล้วทำการเลือกแท็บ Security -> AAA Servers จากนั้นทำการเปิดใช้งาน Authentication และ Accounting Servers ที่ได้มีการเพิ่มเอาไว้แล้ว ดังรูปที่ 3.38



รูปที่ 3.38 การเปิดใช้งาน RADIUS Server ภายใน WLANs

- จากนั้นไปทำการตั้งค่าให้ WLANs ที่เลือก มีการรับ IP Address ที่แจกมาจาก DHCP Servers ดังรูปที่ 3.39



รูปที่ 3.39 การตั้งค่าให้ WLANs เรียกใช้งาน DHCP Server

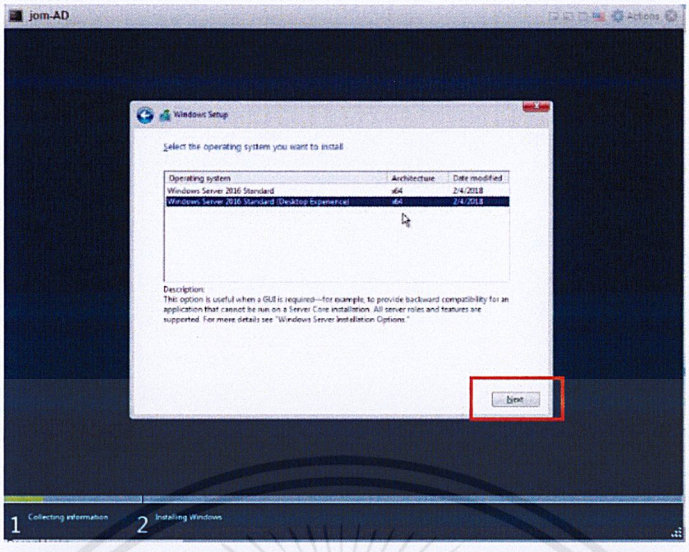
3.3.12. การสร้าง Guest OS ตัวที่ 2 (Active Directory)

ใช้ระบบปฏิบัติการWindows Server 2016 โดยมีขั้นตอนการสร้างคล้ายกับการสร้าง Guest OS ในขั้นตอนที่ 3.3.6 โดยกำหนดให้มีการตั้งค่า Hardware Settings ตามตารางที่ 3.5

CPU	2 CPUs
Memory	8 GB
Harddisk	50 GB
Network Adapter 1	VM Network
Network Adapter 2	internet
CD/DVD Drive	Datastore1/en_windows_server_2016.iso

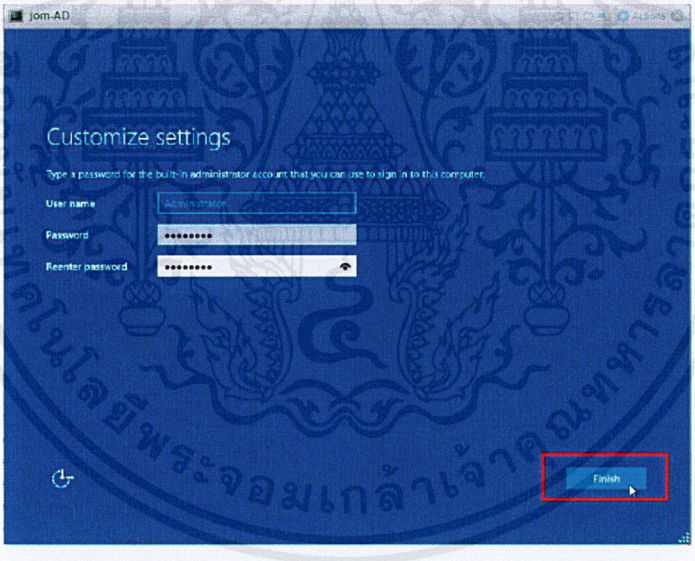
ตารางที่ 3.5 Hardware Settings ของ Guest OS ตัวที่ 2

- จากนั้นเมื่อทำการเปิดการทำงานของ Virtual Machine ขึ้นมา ก็จะเป็นการเข้าสู่การติดตั้งระบบปฏิบัติการ โดยในที่นี้ให้ทำการติดตั้งเป็นแบบ Desktop Experience ดังรูปที่ 3.40 เนื่องจากจะเป็นการติดตั้งให้มีหน้า GUI ที่ใช้งานง่ายทำให้ง่ายต่อการจัดการ



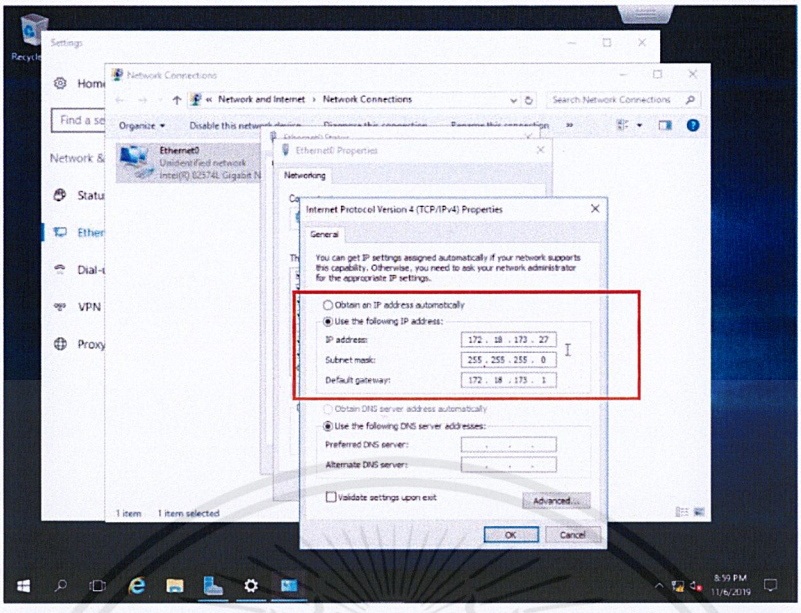
รูปที่ 3.40 การเลือกติดตั้ง Windows Server 2016 Desktop Experience

- เมื่อติดตั้งเสร็จ จะเป็นการเข้าสู่การตั้งค่า Administrator Password ดังรูปที่ 3.41



รูปที่ 3.41 การตั้งค่า Administrator password

- จากนั้นเมื่อทำการเข้าใช้งานด้วย Administrator password ก็จะสามารถทำการตั้งค่าIP Address ของเครื่องได้ โดยให้ทำการตั้งค่าIP Address และ Gateway ของ Ethernet0 เป็น 172.18.173.27 และ 172.18.173.1 ดังรูปที่ 3.42

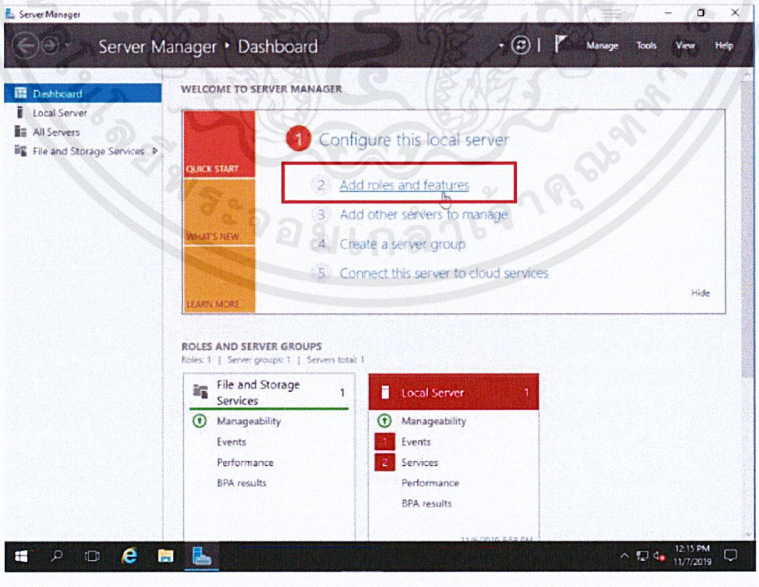


รูปที่ 3.42 การตั้งค่า IP Address ให้กับ Windows Server

3.3.13. การติดตั้ง Active Directory

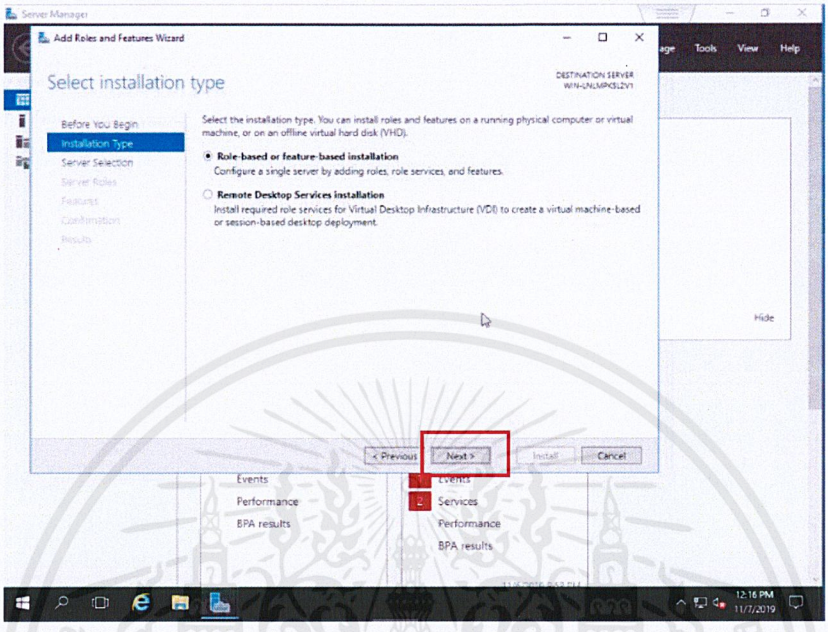
ทำการติดตั้งให้ Windows Server 2016 ทำหน้าที่เป็น Active Directory เพื่อใช้เป็นพื้นที่ในการจัดเก็บข้อมูล

- โดยทำการเข้าสู่ Server Manager และทำการ Add roles and features ดังรูปที่ 3.43

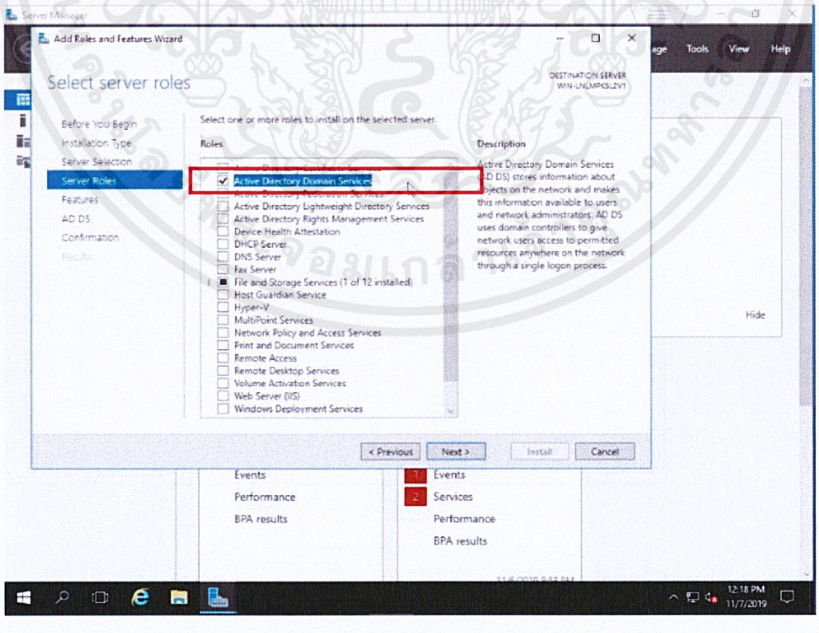


รูปที่ 3.43 การเลือก Add roles and features ให้กับ Window Servers

- โดยให้เลือกติดตั้ง Role-based or feature-based installation แล้วทำการเลือก Server Roles คือ Active Directory Domain Services ดังรูปที่ 3.44 และ 3.45

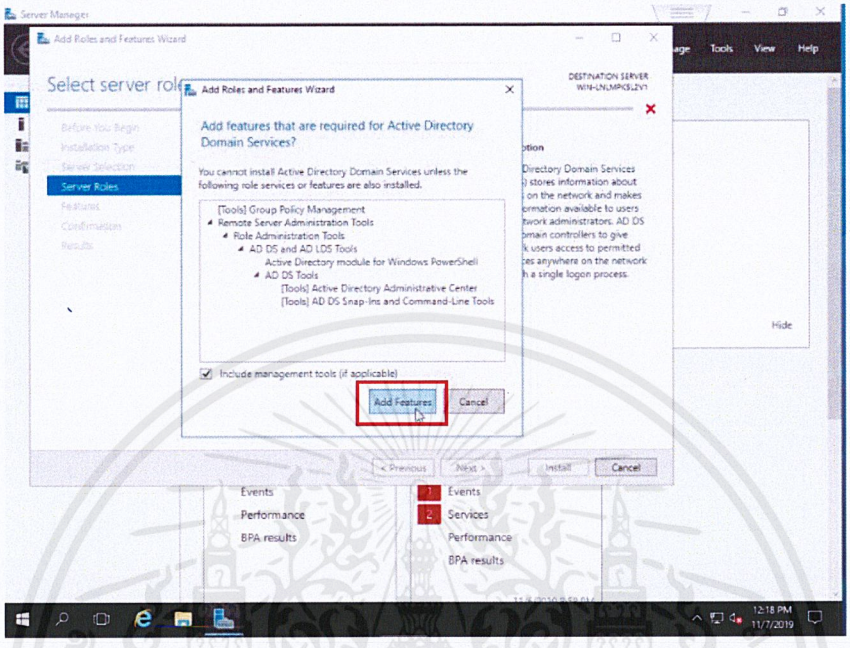


รูปที่ 3.44 การเลือกติดตั้งแบบ Role-based

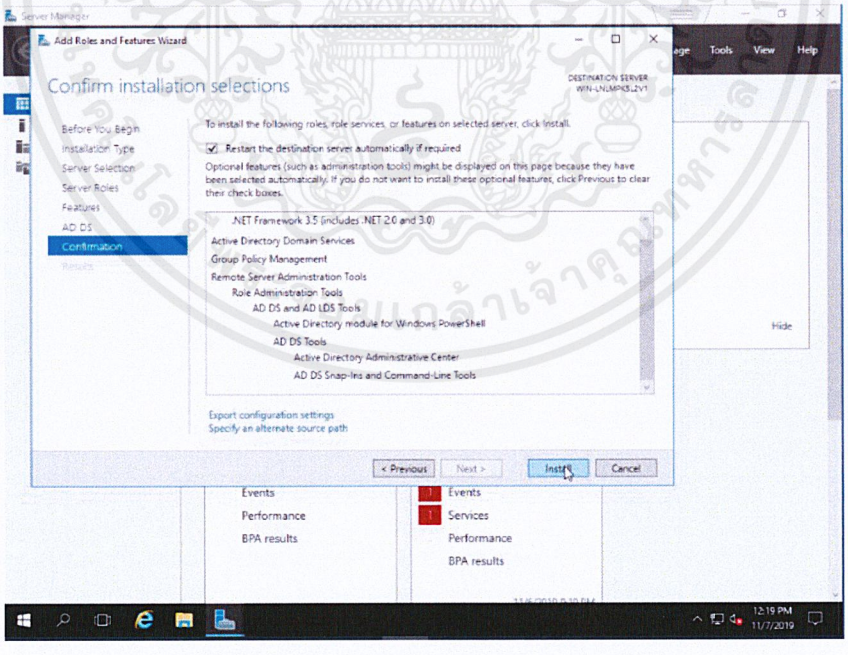


รูปที่ 3.45 การเลือก Roles คือ Active Directory Domian Services

- โดยการเลือกติดตั้ง Active Directory Domain Services ก็อาจต้องทำการติดตั้ง Features อื่นๆเพิ่มเติม ดังรูปที่ 3.46 แล้วจึงทำการตรวจสอบการตั้งค่าก่อนทำการติดตั้ง ดังรูปที่ 3.47

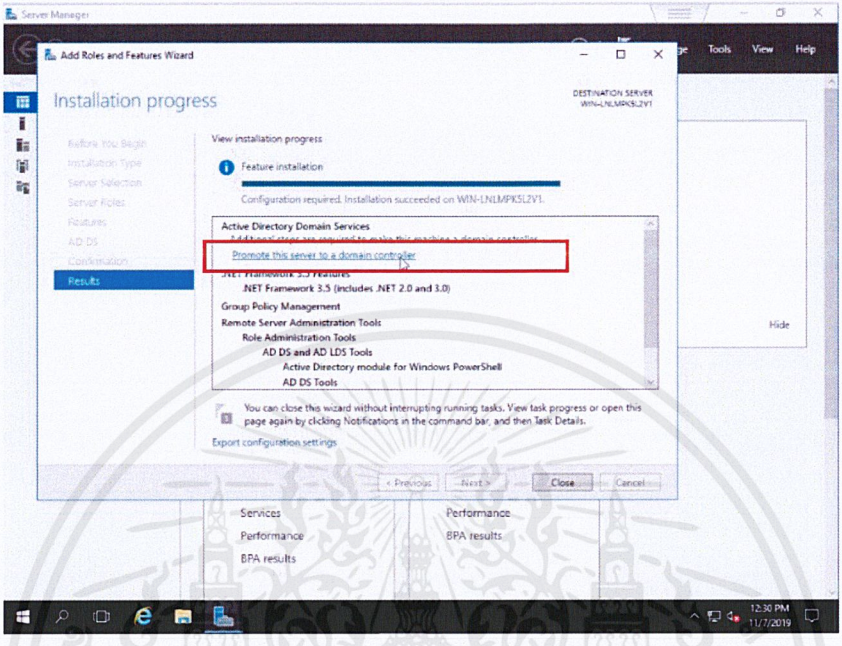


รูปที่ 3.46 การแจ้งเตือนให้มีการติดตั้ง Features อื่นๆเพิ่มเติม



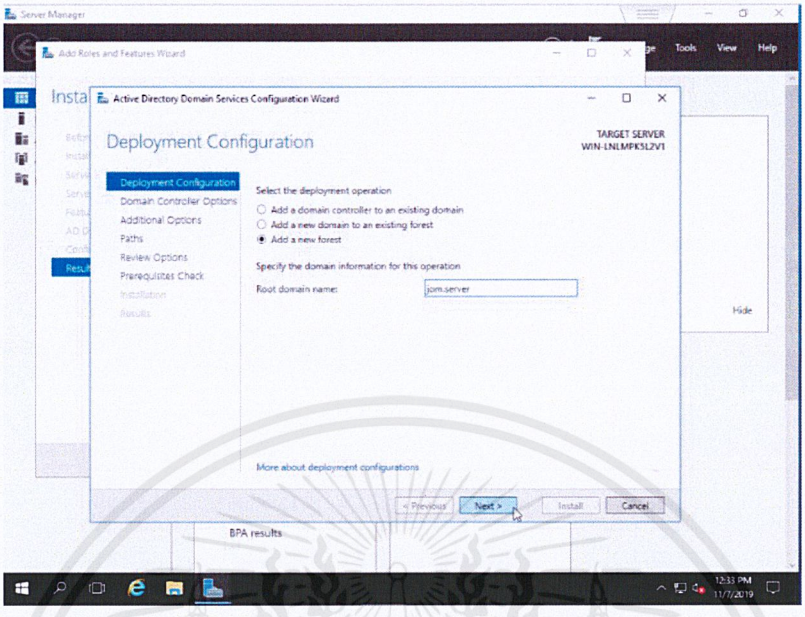
รูปที่ 3.47 การตรวจสอบการตั้งค่าก่อนติดตั้ง

- เมื่อทำการติดตั้งเสร็จเรียบร้อยก็ให้ทำการเลือก Promote this server to a domain controller ดังรูปที่ 3.48 เพื่อให้ Windows Server เครื่องนี้ทำหน้าที่เป็น domain controller

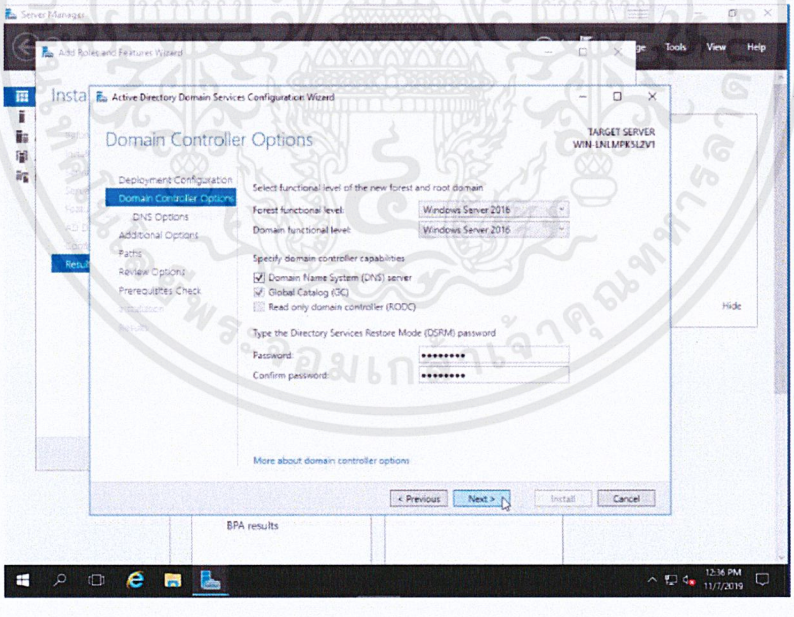


รูปที่ 3.48 การเลือก Promote this server to domain controller

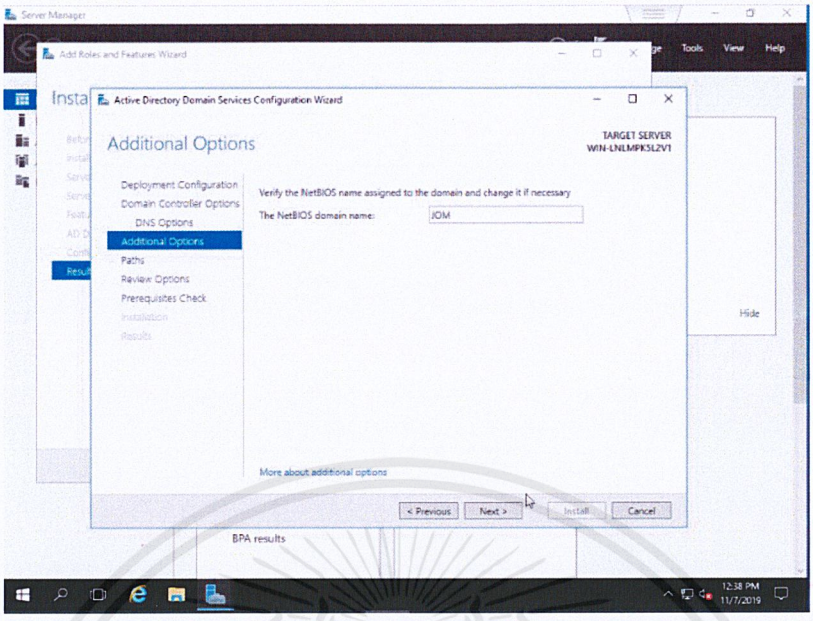
- จากนั้นจะเป็นการตั้งค่าเบื่องต้นของ Domain Controller ได้แก่
    1. ตั้งค่า Deployment Configuration โดยให้ทำการ add a new forest และตั้งชื่อ Root Domain Name ดังรูปที่ 3.49
    2. ตั้งค่า Domain Controller Options ได้แก่ การกำหนด forest และ domain functional level และการกำหนด restore mode password ดังรูปที่ 3.50
    3. ตั้งค่า Additional Options ซึ่งเป็นการตั้งค่า NetBIOS Name ดังรูปที่ 3.51
    4. ตั้งค่า Paths ดังรูปที่ 3.52



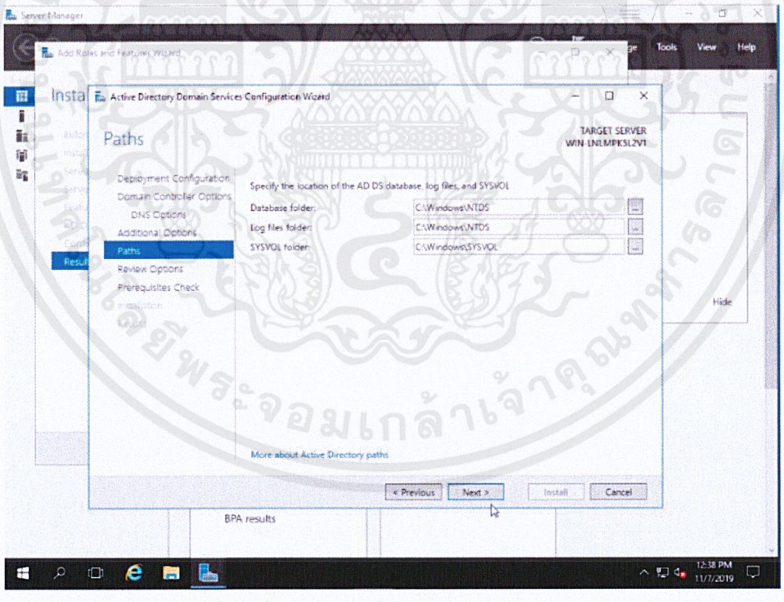
รูปที่ 3.49 การตั้งค่า Deployment Configuration



รูปที่ 3.50 การตั้งค่า Controller Options

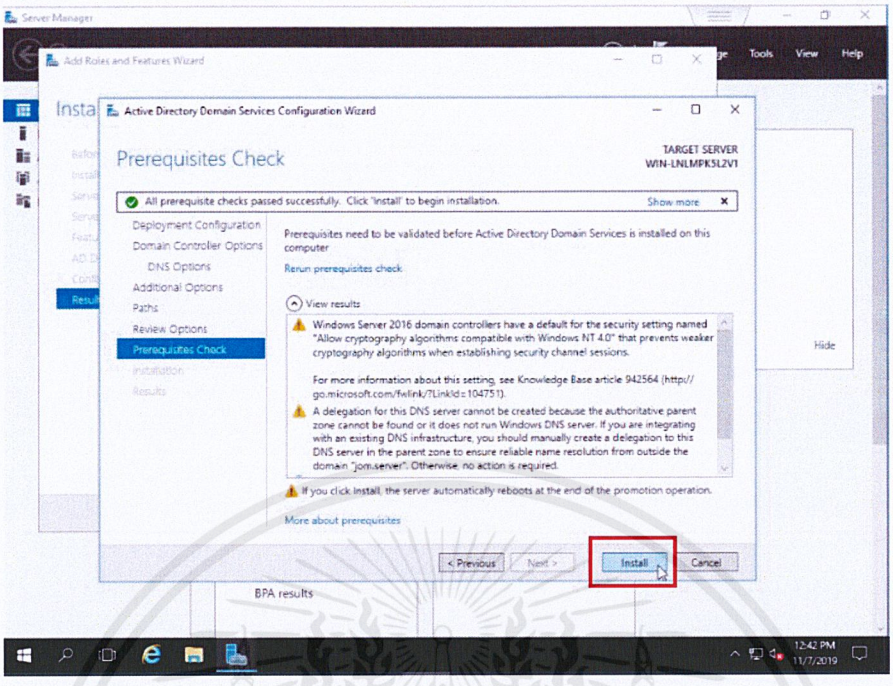


รูปที่ 3.51 การตั้งค่า Additional Options



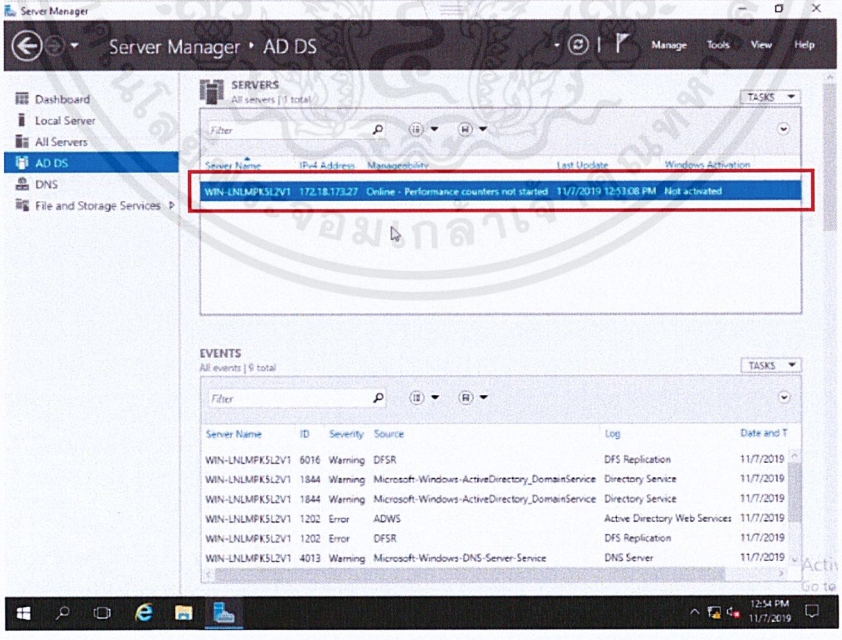
รูปที่ 3.52 การตั้งค่า Paths

- จากนั้นเมื่อทำการตั้งค่าเบื้องต้นให้กับ Domain Controller เสร็จเรียบร้อย ก็จะทำการ Prerequisites Checks ก่อนจะเข้าสู่การติดตั้งดังรูปที่ 3.53



รูปที่ 3.53 การ Prerequisites Checks ก่อนเข้าสู่การติดตั้ง

- เมื่อทำการติดตั้งเสร็จเรียบร้อย ก็สามารถเข้าไปตรวจสอบได้โดยเข้าไปที่ Server Manager -> AD DS แล้วดูรายชื่อและ IP Address ของเครื่องที่ทำหน้าที่เป็น Domain Controller ดังรูปที่ 3.54

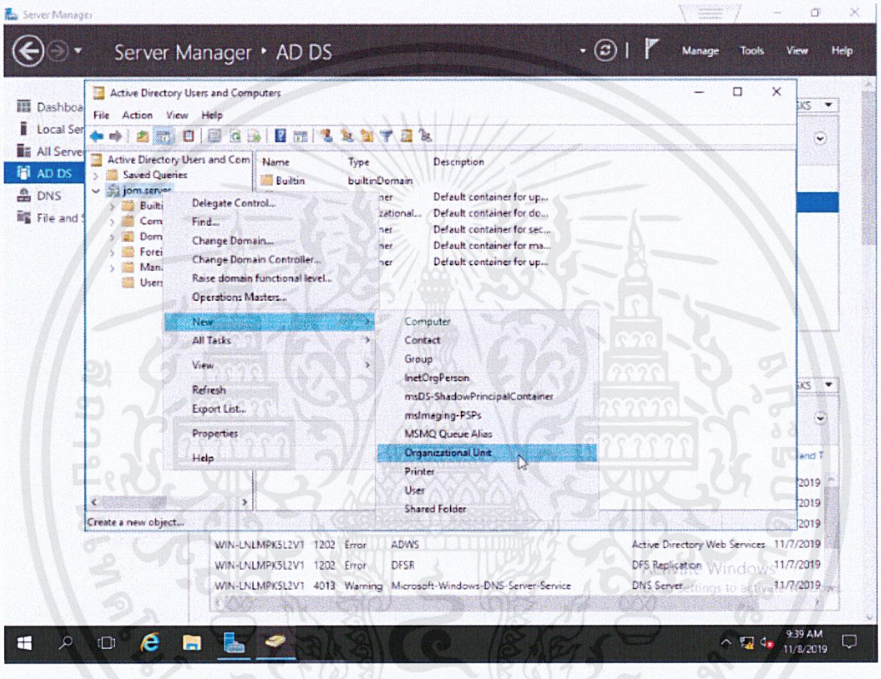


รูปที่ 3.54 IP Address ของ Domain Controller

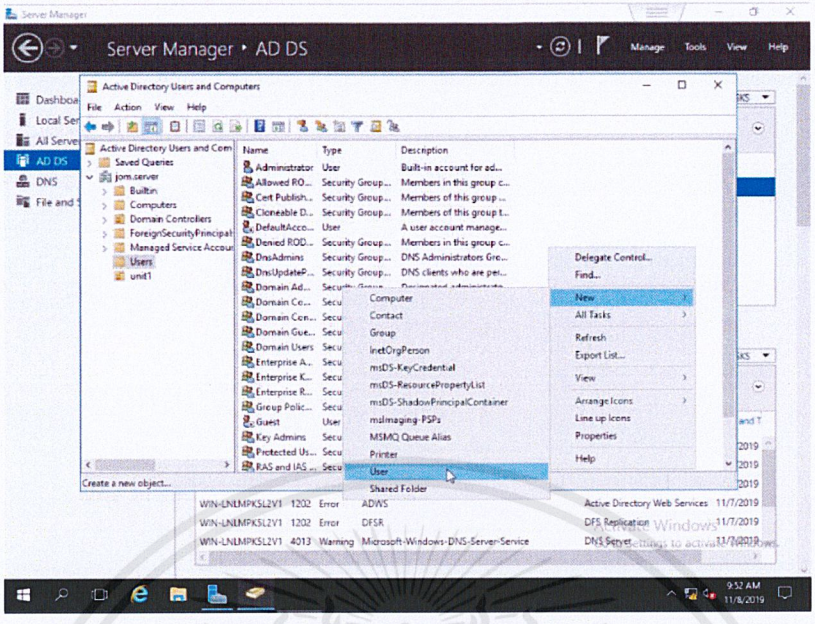
3.3.14. การสร้าง Organization Unit และบัญชีผู้ใช้งานมีบทบาทเป็นผู้ดูแลระบบ

โดยสร้าง Organization Unit สำหรับใช้เสมือนเป็นพื้นที่จัดเก็บข้อมูลของบัญชีผู้ใช้ภายในองค์กรโดยใช้ชื่อว่า unit1 และทำการสร้างบัญชีผู้ใช้งานโดยใช้ชื่อว่า calladmin เพื่อให้มีบทบาทเป็น Administrator ที่สามารถจัดการภายใน Organization Unit ได้

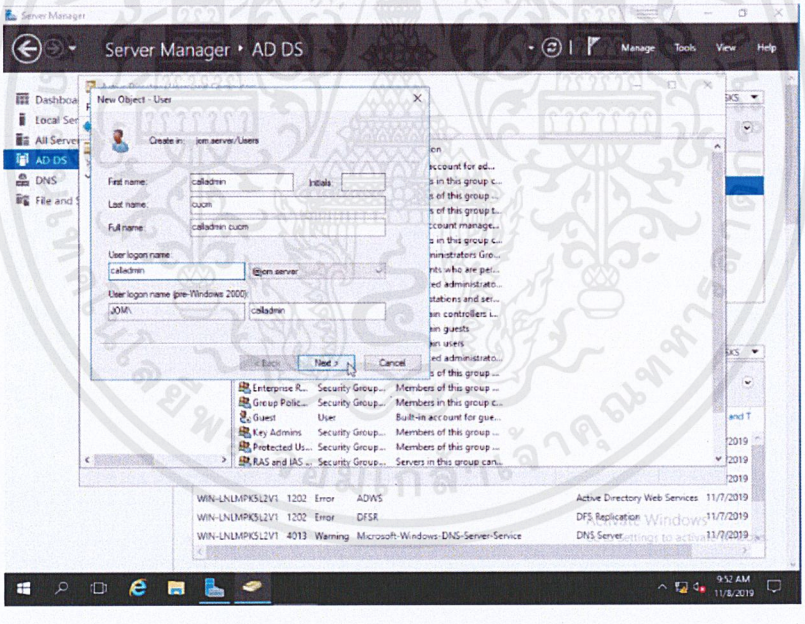
- โดยเข้าไปที่ Active Directory Users and Computers/jom.server แล้วทำการสร้าง New -> Organization Unit และ New -> Users ดังรูปที่ 3.55, 3.56 และ 3.57



รูปที่ 3.55 การสร้าง Organization Unit

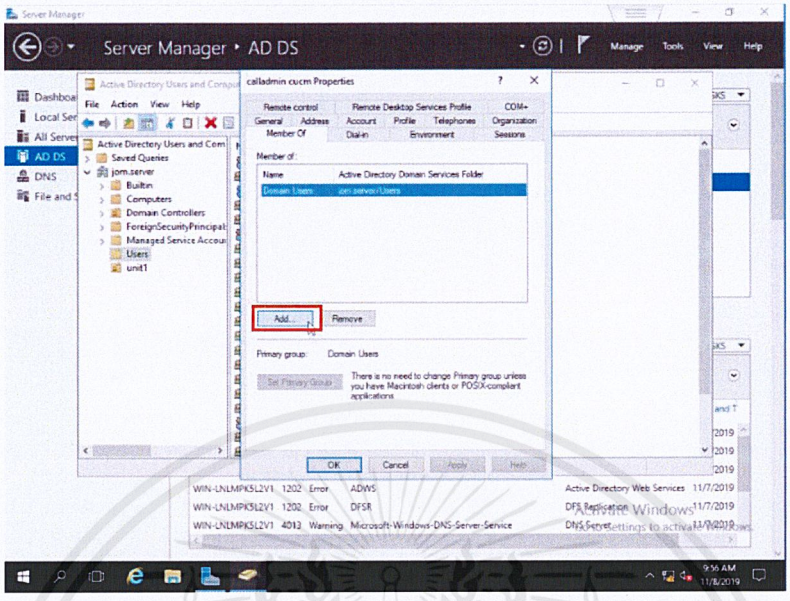


รูปที่ 3.56 การสร้างบัญชีผู้ใช้งาน 1

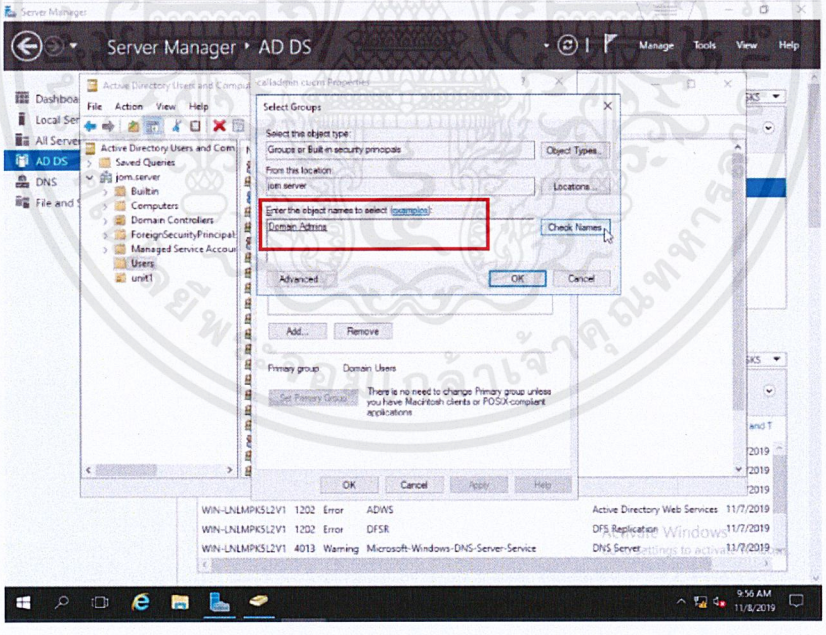


รูปที่ 3.57 การสร้างบัญชีผู้ใช้งาน 2

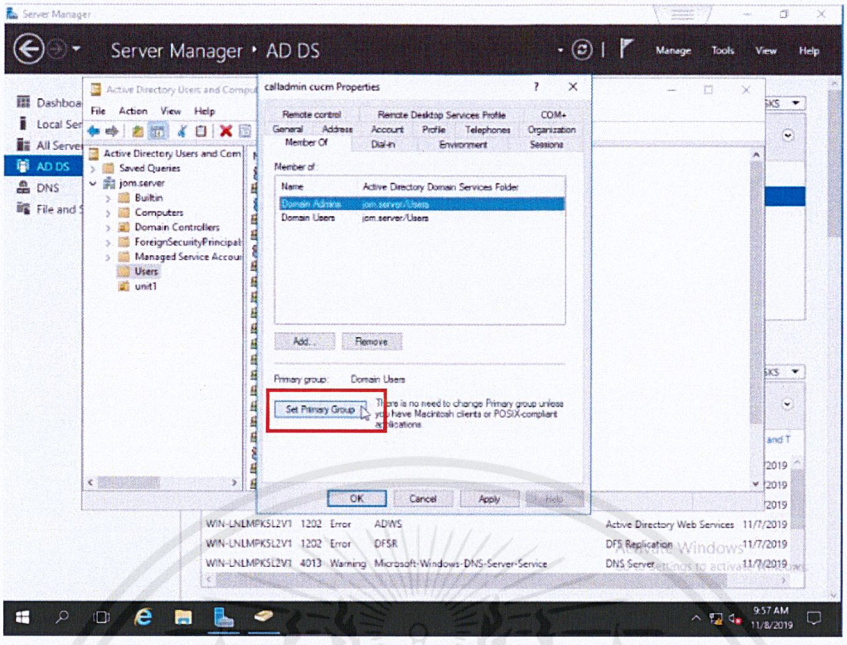
- ทำการกำหนดสิทธิ์ในการเป็น Administrator เพื่อให้สามารถทำการจัดการ unit1 ให้กับ calladmin โดยคลิกขวาที่ชื่อ calladmin แล้วเลือกไปที่ Properties จากนั้นทำการเพิ่ม User นี้ ให้เป็นสมาชิกของ Domain Admin แล้วตั้งค่าให้ Domain Admin เป็นบทบาทหลักของ Users นี้ ตามรูปที่ 3.58 ,3.59 และ 3.60 ตามลำดับ



รูปที่ 3.58 การกำหนดให้ calladmin เป็นสมาชิกของ Domain Administrator 1

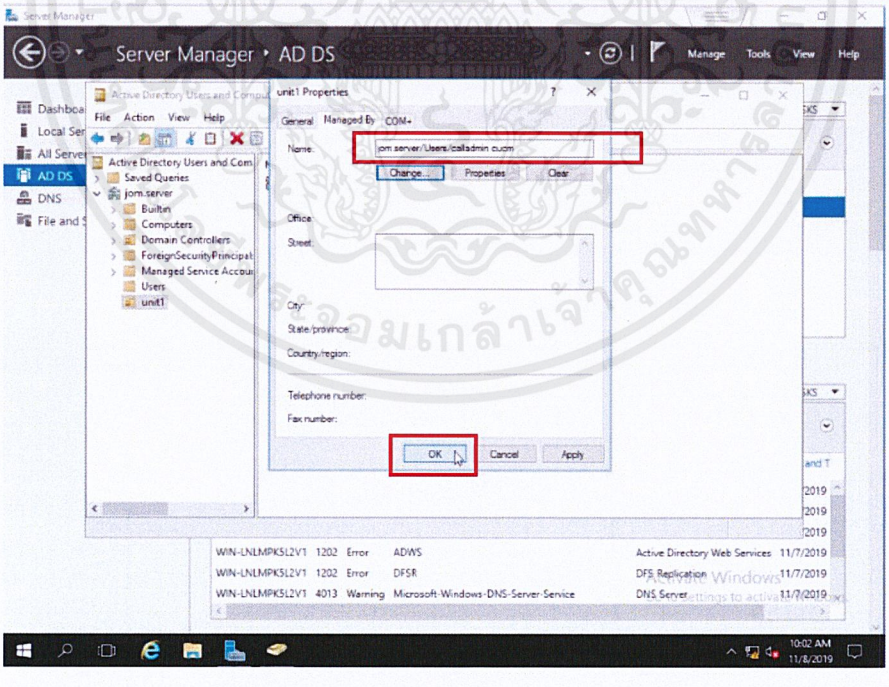


รูปที่ 3.59 การกำหนดให้ calladmin เป็นสมาชิกของ Domain Administrator 2



รูปที่ 3.60 การตั้งค่าให้ Domain Admin เป็นบทบาทหลัก

- จากนั้นทำการเพิ่มสิทธิ์ผู้ที่สามารถจัดการภายใน Organization Unitได้ โดยไปที่ unit1 -> Properties -> Managed By แล้วทำการเปลี่ยน Name: เป็น calladmin ดังรูปที่ 3.61



รูปที่ 3.61 การเพิ่มชื่อของผู้ที่มีมิทธิ์ในการจัดการ Organization Unit

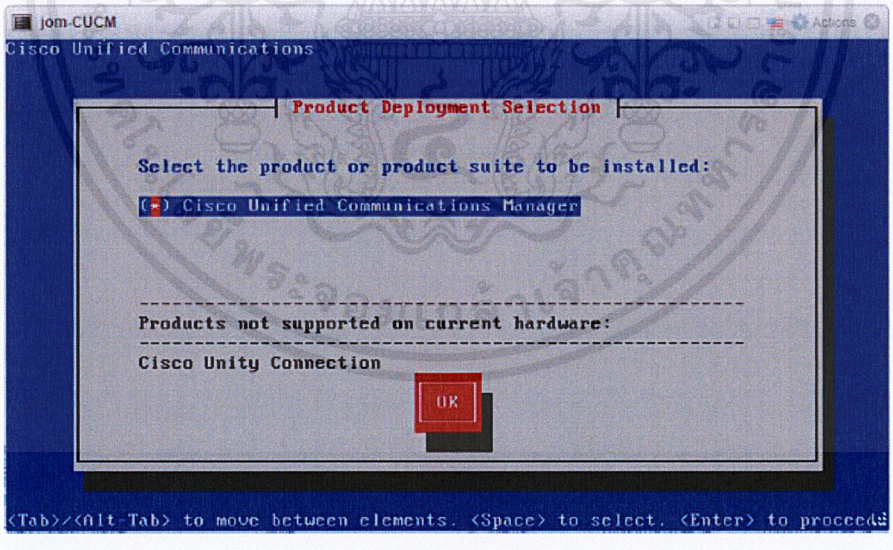
3.3.15. การสร้าง Guest OS ตัวที่ 3 (Call Manager)

ทำการติดตั้ง Cisco Unified Communications Manager (CUCM) เพื่อใช้สำหรับจัดการระบบการสื่อสารผ่านระบบโทรศัพท์ IP Phone โดยกำหนด Hardware Settings ตามตารางที่ 3.6

ตารางที่ 3.6 Hardware Settings ของ Guest OS ตัวที่ 3

CPU	4 CPUs
Memory	16 GB
Harddisk	80 GB
Network Adapter 1	VM Network
Network Adapter 2	internet
CD/DVD Drive	Datastore1/ UCSInstall_UCOS_11.5.1.16900-16.sgn

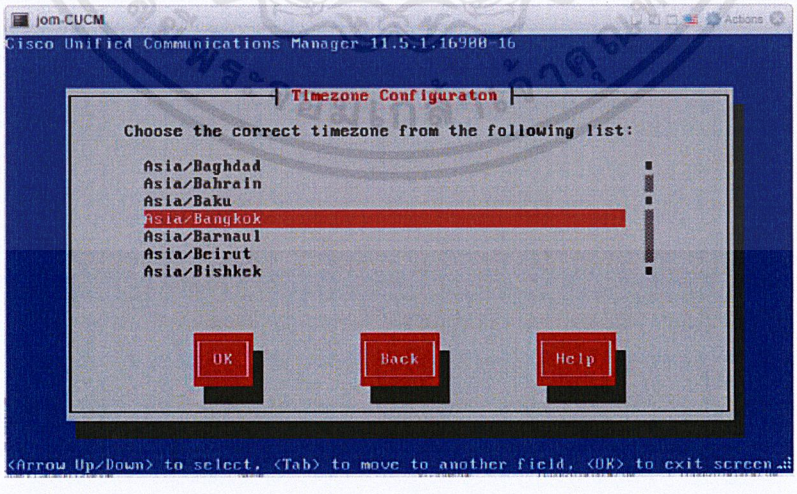
- เมื่อทำการเปิดการทำงานของ Virtual Machine ขึ้นมา ก็จะเป็นการเข้าสู่ขั้นตอนติดตั้งระบบ โดยให้ทำการเลือกติดตั้ง Cisco Unified Communications Manager ดังรูปที่ 3.62



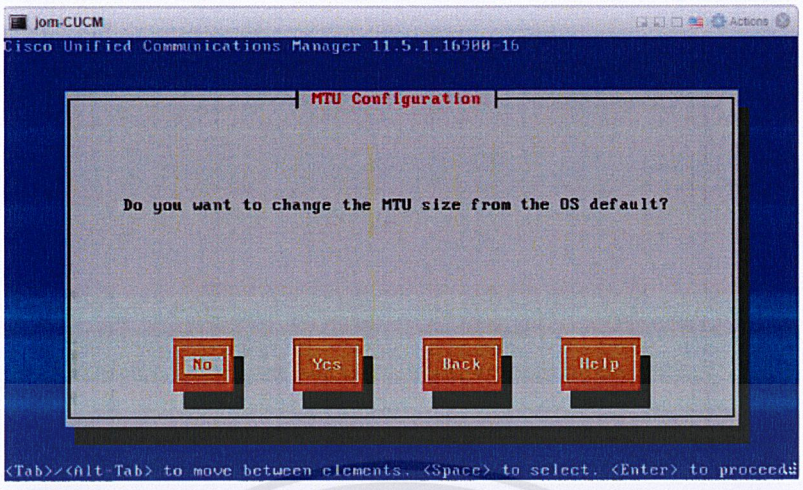
รูปที่ 3.62 การเลือกติดตั้ง CUCM

- จากนั้นจะเป็นการเข้าสู่การตั้งค่าพื้นฐานให้กับ CUCM ซึ่งมีการตั้งค่าที่จำเป็นได้แก่

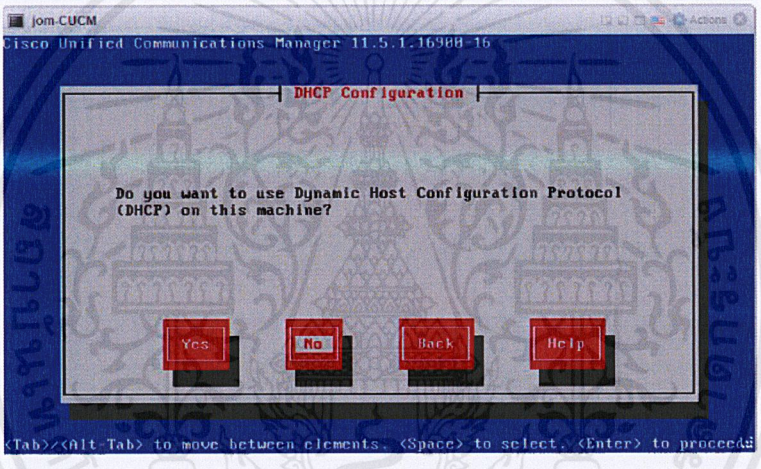
1. การตั้งค่า Timezone Configuration โดยเลือกเป็น Asia/Bangkok ดังรูปที่ 3.63
2. การตั้งค่า MTU Size โดยให้ใช้ค่าดั้งเดิม ดังรูปที่ 3.64
3. การตั้งค่าการใช้งาน DHCP ดังรูปที่ 3.65 โดยในที่นี้ยังไม่เปิดใช้งาน
4. การตั้งค่า Network Configuration ได้แก่ การตั้งค่า Hostname, IP Address และ Gateway ดังรูปที่ 3.66
5. การตั้งค่า DNS Client ดังรูปที่ 3.67 โดยในที่นี้ยังไม่เปิดใช้งาน
6. การตั้งค่า Administration Login ซึ่งได้แก่การตั้งค่า Password สำหรับการเข้าจัดการ ดังรูปที่ 3.68
7. การตั้งค่า Certificate Information คือการเพิ่มข้อมูลเบื้องต้นขององค์กร ดังรูปที่ 3.69
8. การตั้งค่า NTP Server ให้ชี้ไปยังGuest OS ตัวที่1 ดังรูปที่ 3.70
9. การตั้งค่าSecurity Password สำหรับใช้ในการสื่อสารกันระหว่าง Cluster node ดังรูปที่ 3.71
10. การตั้งค่า Smart Call Home โดยยังไม่มีการใช้งานในส่วนนี้ ดังรูปที่ 3.72
11. การตั้งค่า Application User เพื่อการเข้าใช้งานการจัดการผ่านหน้าเว็บได้ โดยตั้งค่าดังรูปที่ 3.73



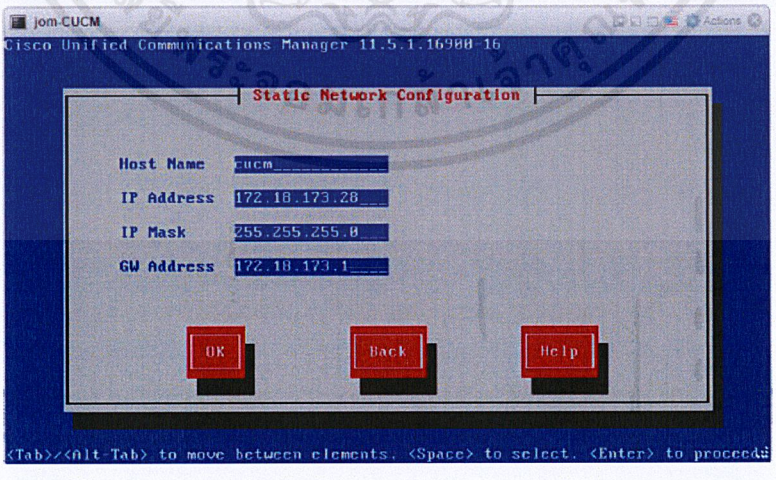
รูปที่ 3.63 การตั้ค่า Timezone Configuration



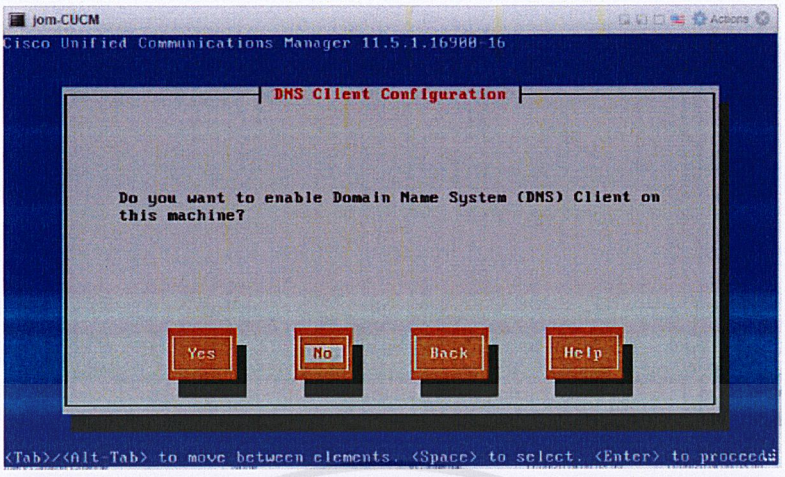
รูปที่ 3.64 การตั้งค่า MTU Configuration



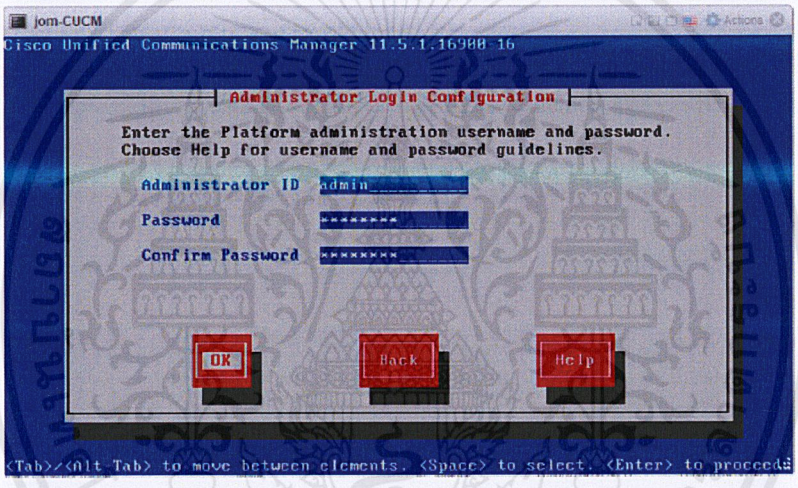
รูปที่ 3.65 การตั้งค่า DHCP Configuartion



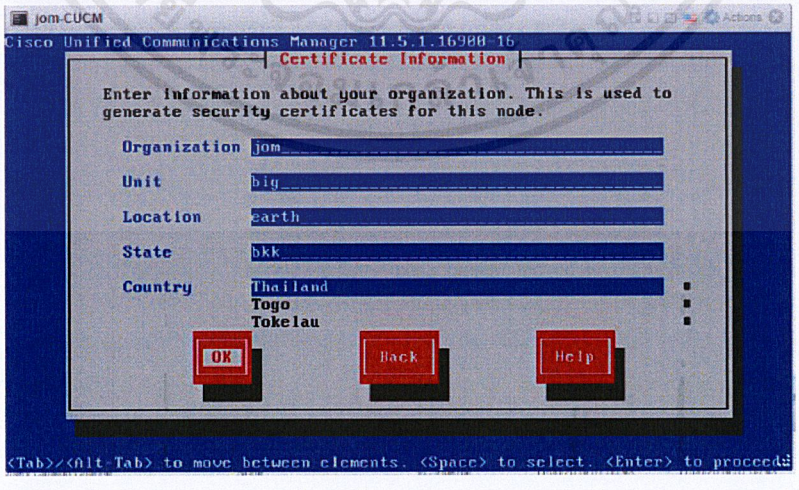
รูปที่ 3.66 การตั้งค่า Network Configuration



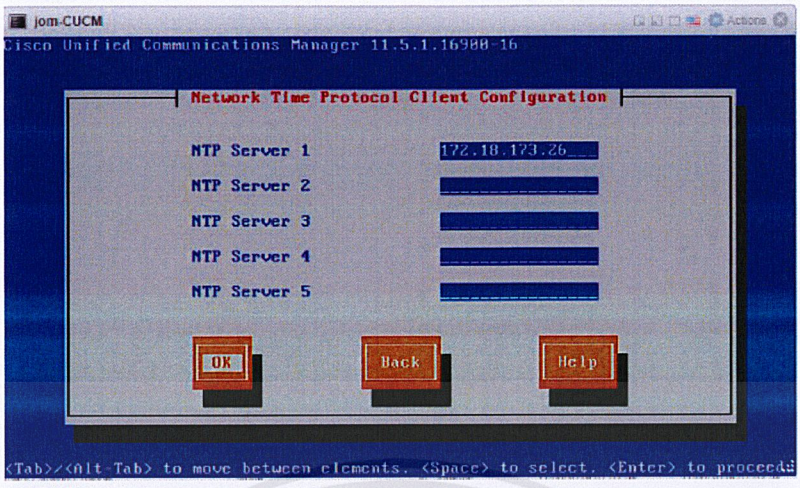
รูปที่ 3.67 การตั้งค่า DNS Client Configuration



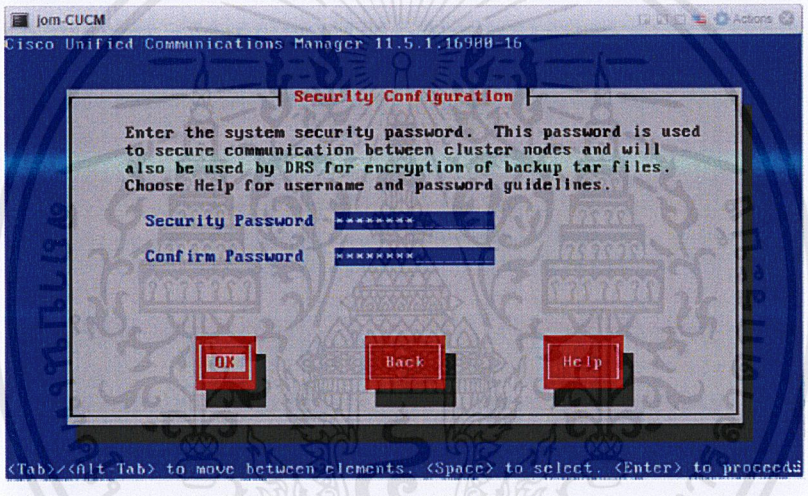
รูปที่ 3.68 การตั้งค่า Administrator Login



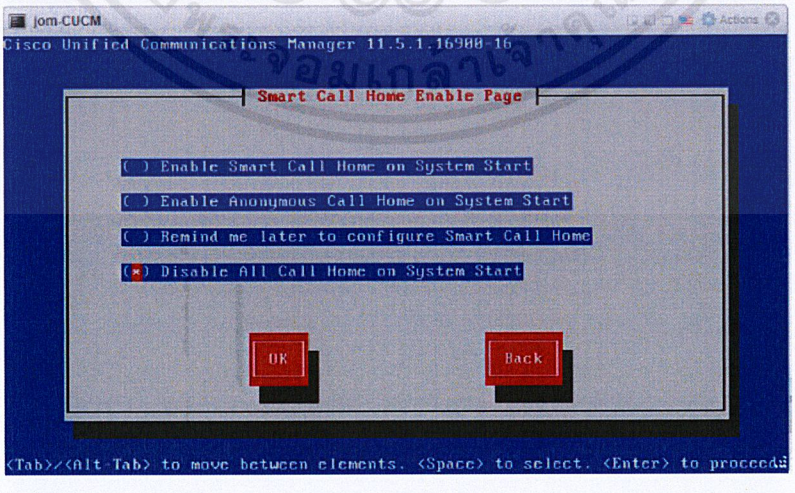
รูปที่ 3.69 การตั้งค่า Certificate Information



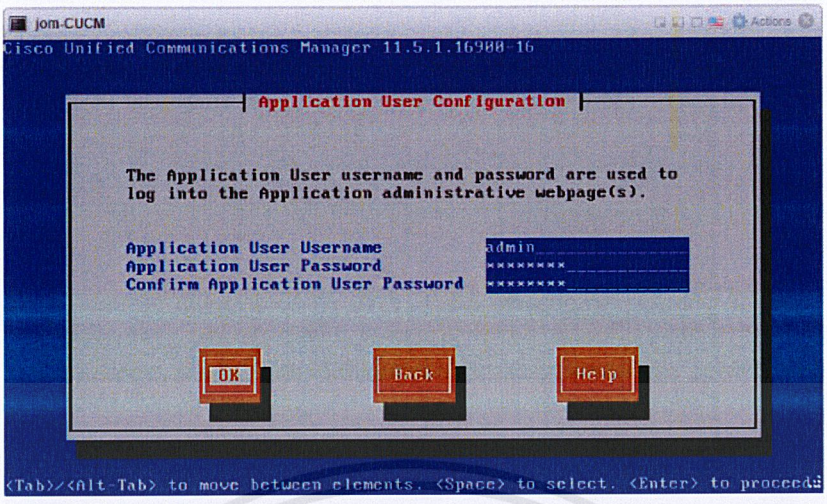
รูปที่ 3.70 การตั้งค่า NTP Client Configuration



รูปที่ 3.71 การตั้งค่า Security Password

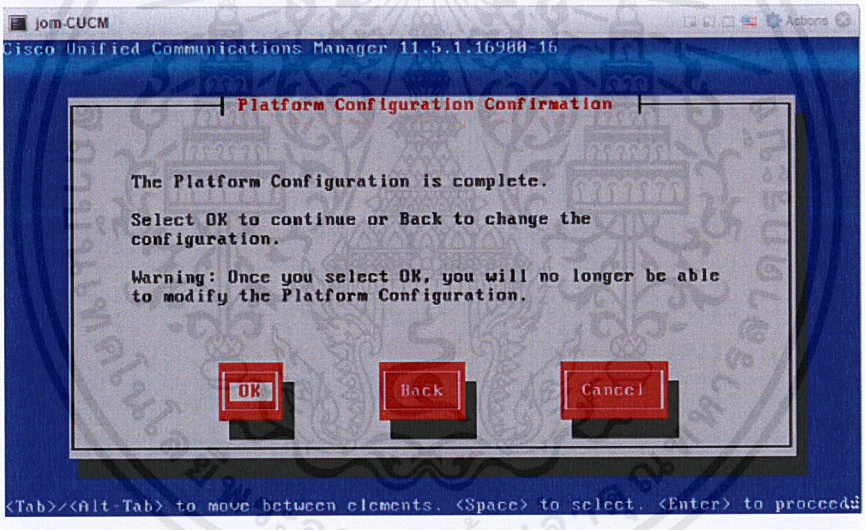


รูปที่ 3.72 การกำหนด Smart Call Home



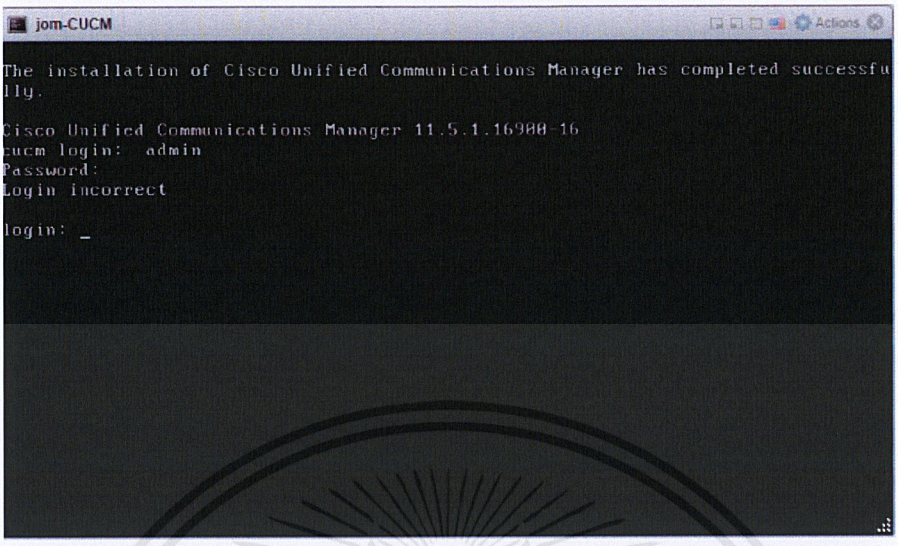
รูปที่ 3.73 การตั้งค่า Application User

- หลังจากทำการตั้งค่าเสร็จสิ้น ให้กด OK เพื่อทำการเข้าสู่กระบวนการติดตั้งต่อไป



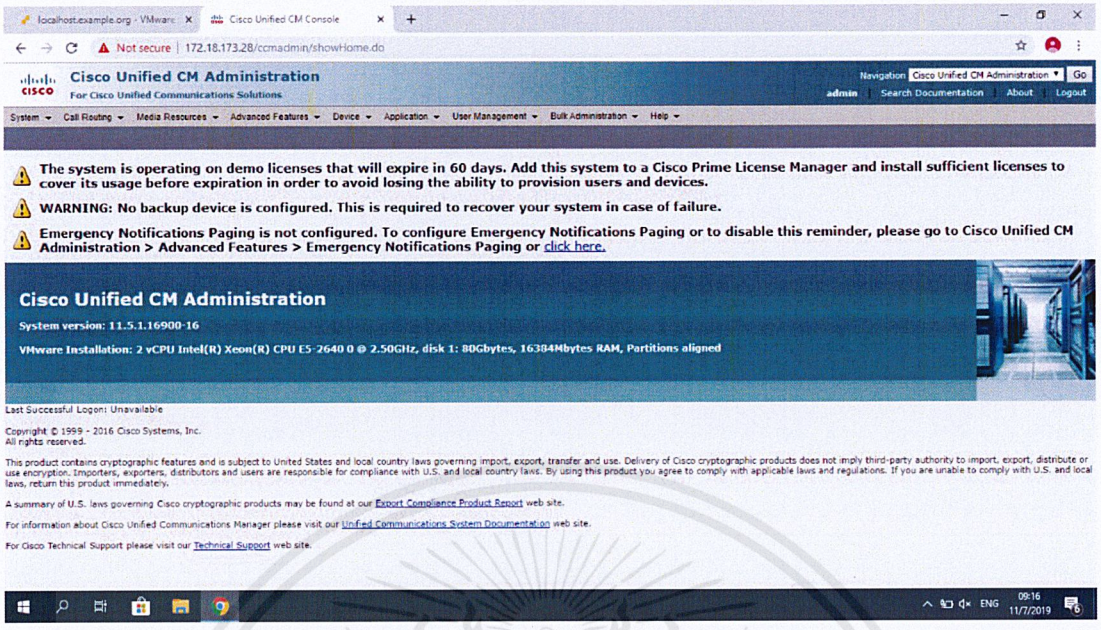
รูปที่ 3.74 หน้าจอแสดงผลว่าการตั้งค่าเสร็จสมบูรณ์พร้อมทำการติดตั้งต่อ

- เมื่อทำการติดตั้งเสร็จ CUCM จะทำการ Restart ตัวเองก่อน แล้วจึงจะสามารถเข้าใช้งานได้ ทั้งการเข้าใช้งานผ่านหน้า Console ของ Virtual Machine และเข้าใช้งานผ่านหน้าเว็บด้วย IP Address ที่ตั้งไว้คือ 172.18.173.28 ดังรูปที่ 3.75, 3.76 และ 3.77



รูปที่ 3.75 การ Login เข้าใช้งาน CUCM ผ่านหน้า Console

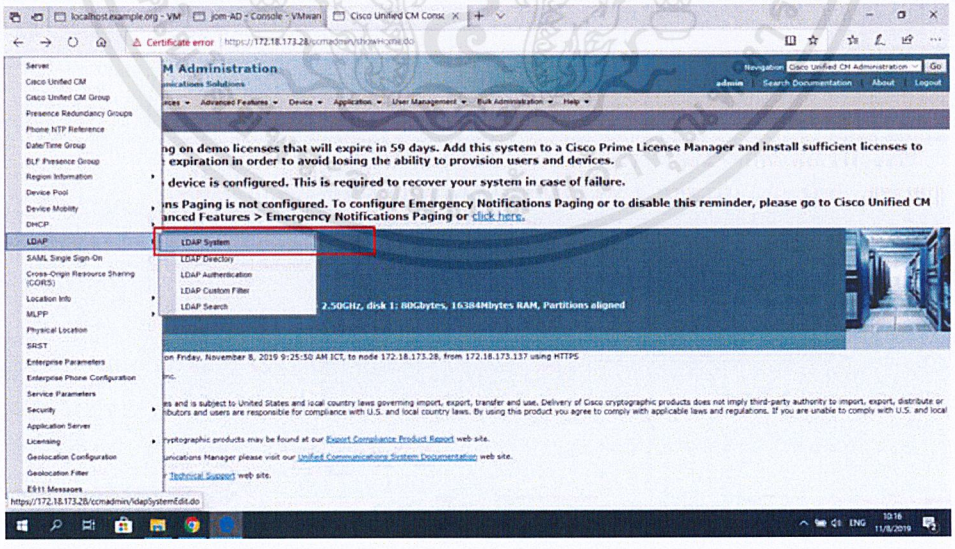
รูปที่ 3.76 การเข้าใช้งาน CUCM ผ่านหน้าเว็บ 1



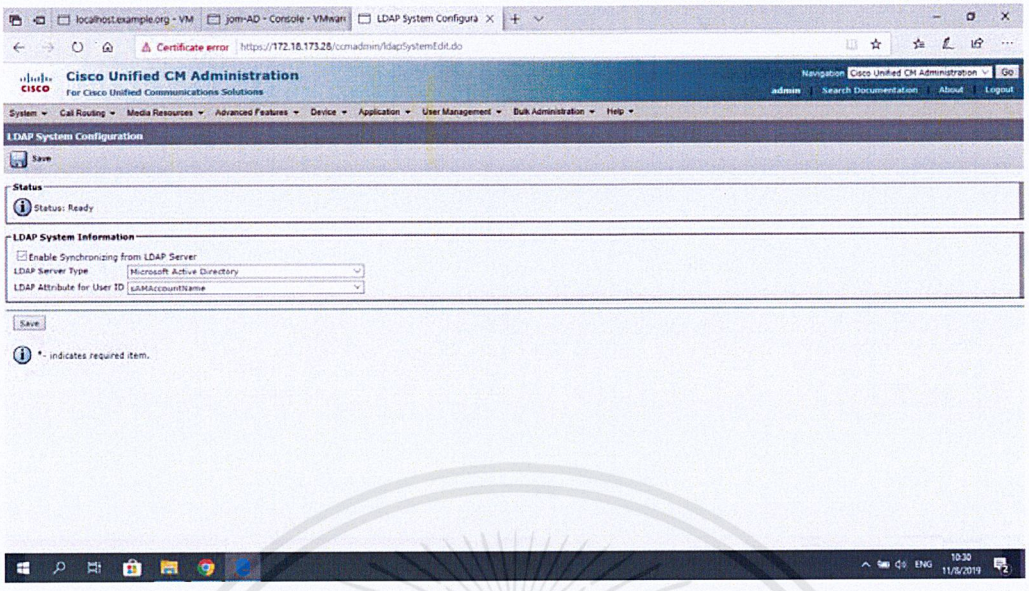
รูปที่ 3.77 การเข้าใช้งาน CUCM ผ่านหน้าเว็บ 2

3.3.16. การติดตั้งและทดสอบระบบโทรศัพท์ IP Phone

- ทำการสร้าง LDAP System และ LDAP Directory สำหรับกำหนดให้ CUCM ดึงข้อมูลจาก Active Directory โดยเข้าไปที่ Cisco Unifiem CM Administration -> Systems -> LDAP -> LDAP Systems และทำการเปิดการทำงานของ LDAP Systems ดังรูปที่ 3.78

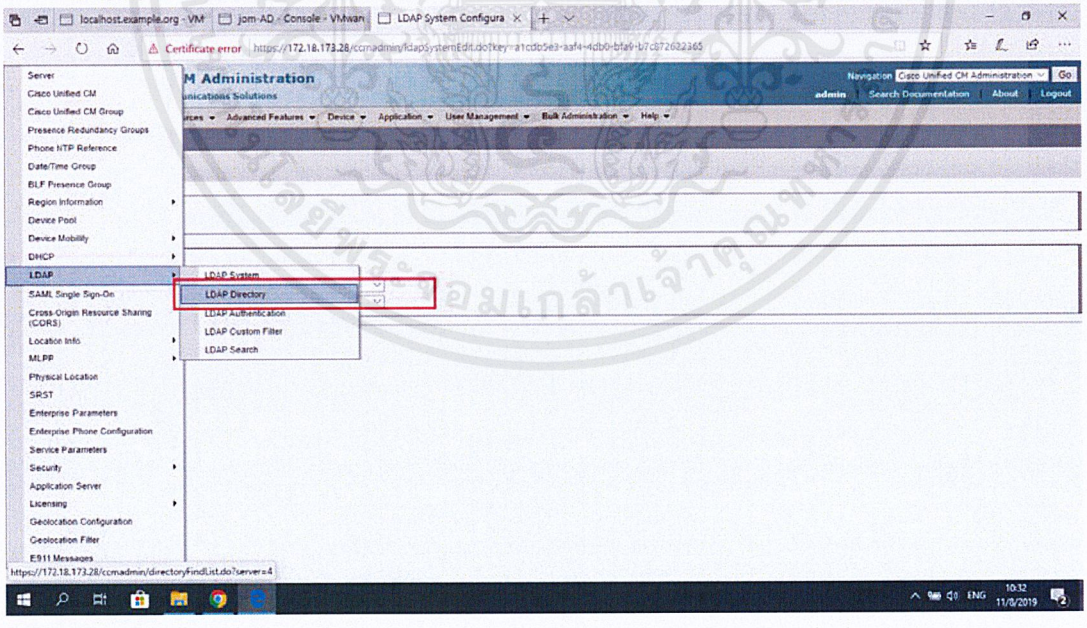


รูปที่ 3.78 การเปิดใช้งาน LDAP Systems 1

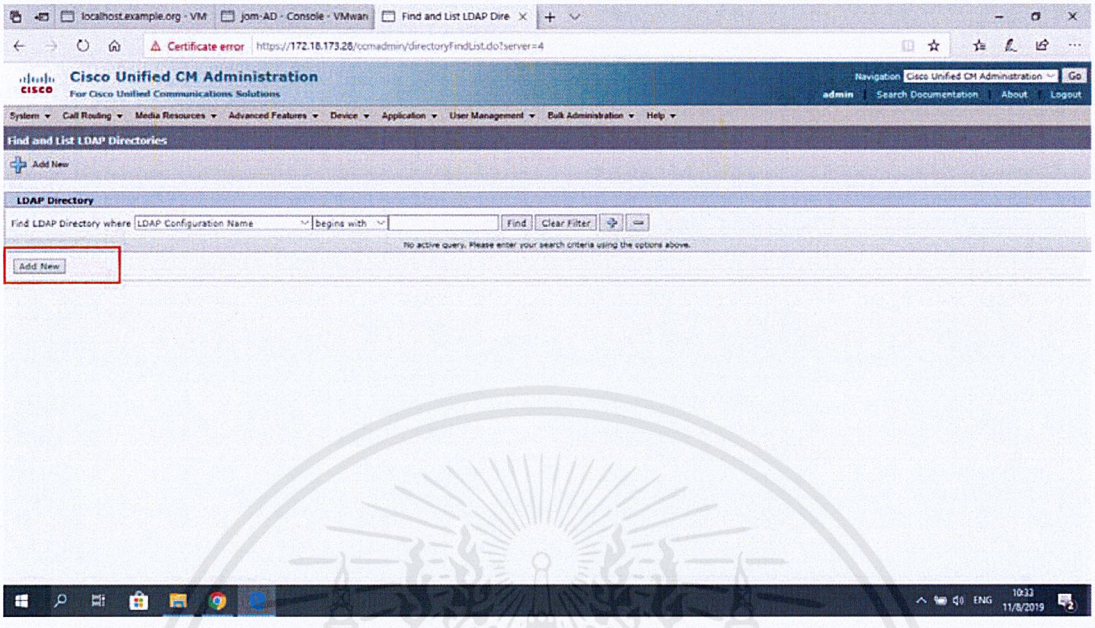


รูปที่ 3.79 การเปิดใช้งาน LDAP Systems 2

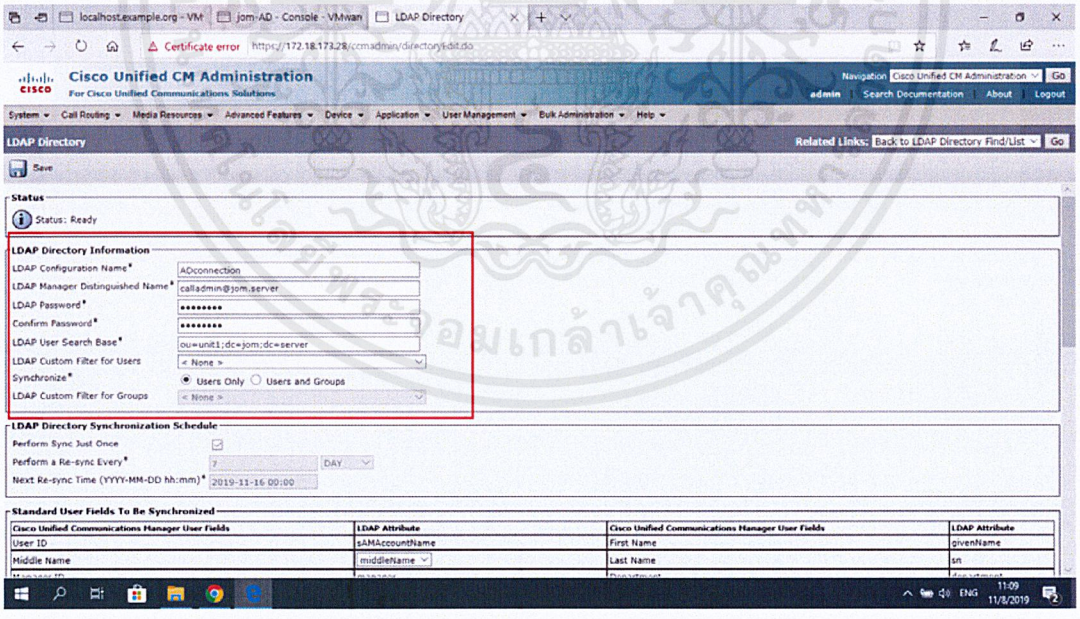
- จากนั้นจึงทำการสร้าง LDAP Directory ที่มีการชี้ไปยัง Active Directory โดยเข้าไปยัง Cisco Unifiem CM Administration -> Systems -> LDAP -> LDAP Directory และทำการเพิ่ม LDAP Directory ดังรูปที่ 3.80 และ 3.81 แล้วทำการตั้งค่าดังรูปที่ 3.82 และ 3.83



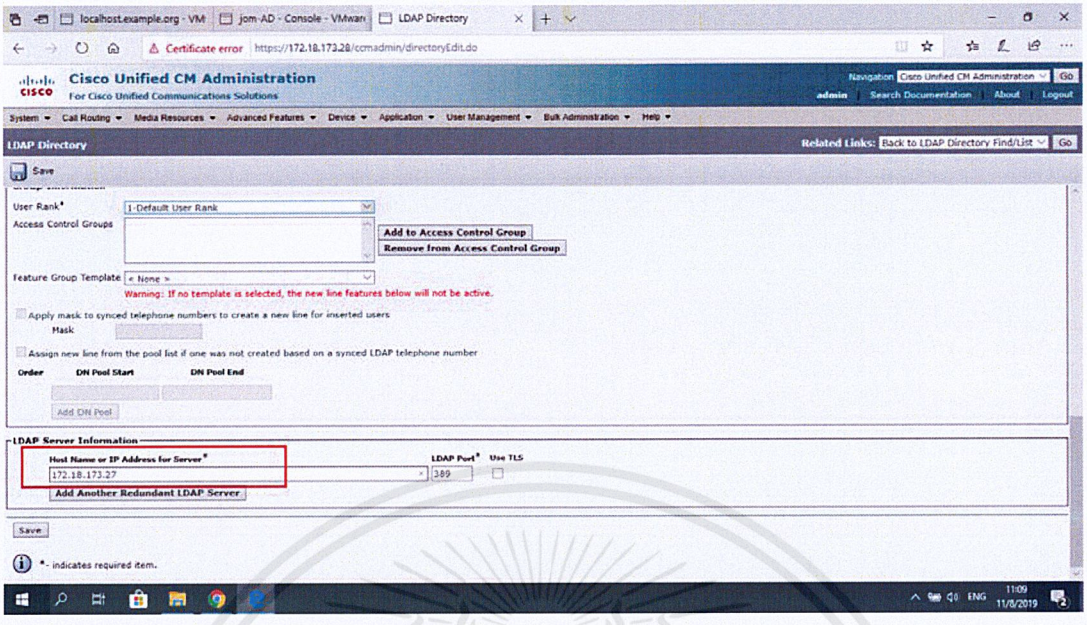
รูปที่ 3.80 การสร้าง LDAP Directory 1



รูปที่ 3.81 การสร้าง LDAP Directory 2

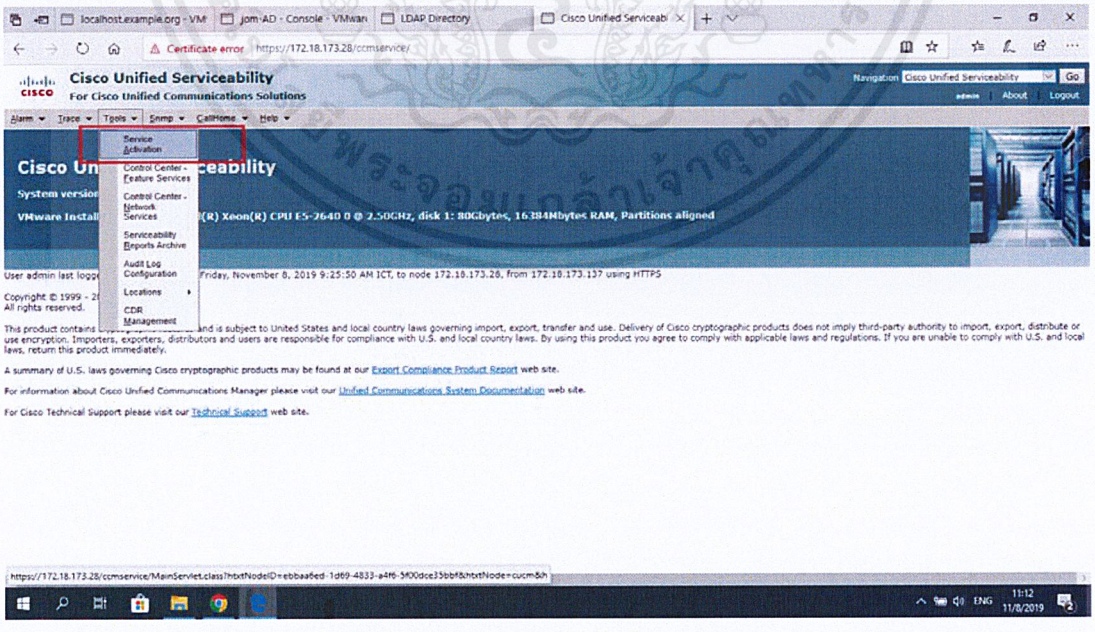


รูปที่ 3.82 การตั้งค่า LDAP Directory 1



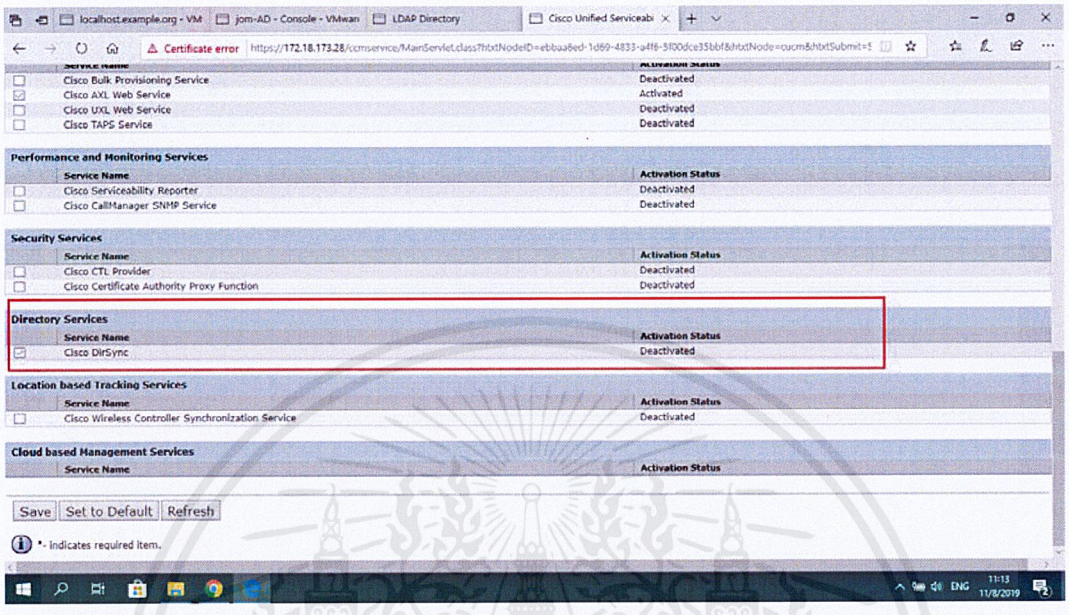
รูปที่ 3.83 การตั้งค่า LDAP Directory 2

- ทำการเปิดใช้งาน Service ที่จำเป็น ได้แก่ Cisco DirSync ซึ่งทำให้สามารถดึงข้อมูลจากActive Directory มาได้ และ Cisco TFTP ซึ่งทำให้สามาถส่งข้อมูลการตั้งค่าไปยังโทรศัพท์แต่ละเครื่องในระบบได้ โดยเข้าไปที่ Cisco Unified Serviceability -> Tools -> Service Activation ดังรูปที่ 3.84

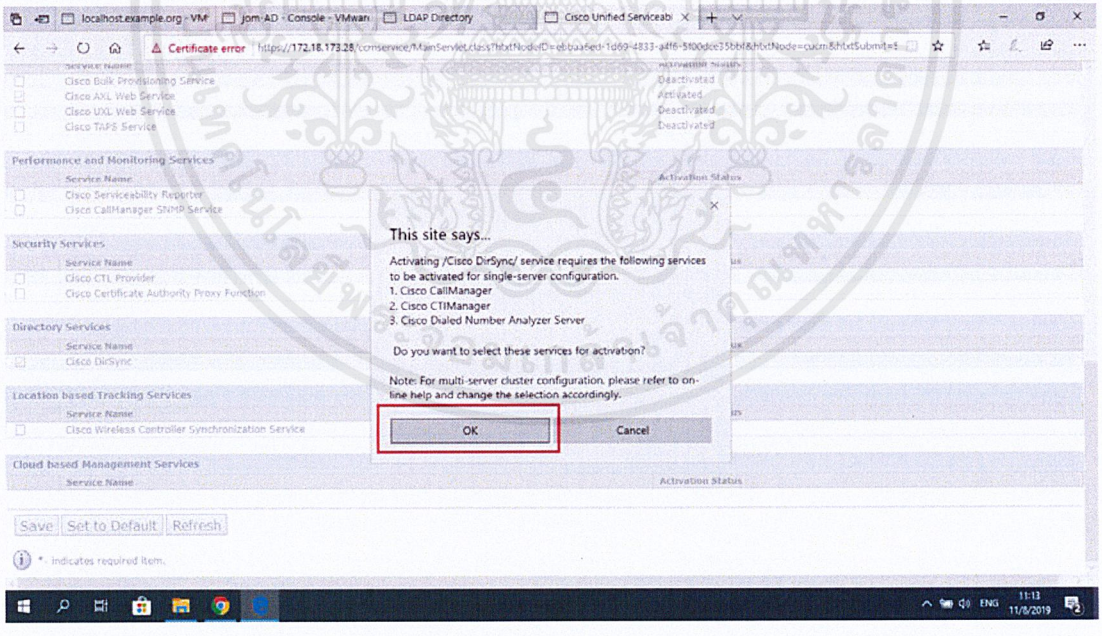


รูปที่ 3.84 การเข้าสู่ Service Activation

- ทำการเลือกเปิดใช้งาน Cisco DirSync ซึ่งระบบจะแจ้งเตือนเพื่อให้เปิดใช้งานService อื่นๆที่เกี่ยวข้องด้วยก็ให้ทำการตกลงไป ดังรูปที่ 3.85 และ 3.86

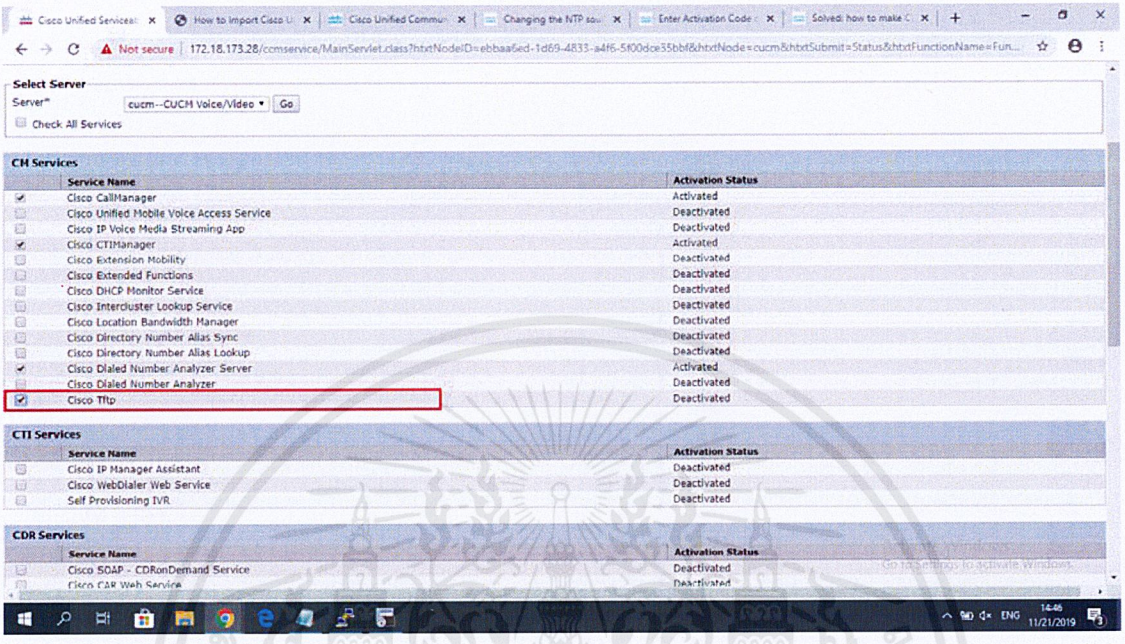


รูปที่ 3.85 การเปิดใช้งาน Cisco DirSync



รูปที่ 3.86 การแจ้งเตือนเพื่อไปใช้งาน Services อื่นๆที่เกี่ยวข้อง

- จากนั้นทำการเปิดใช้งาน Cisco TFTP ดังรูปที่ 3.87 หรืออาจเปิดการใช้งานพร้อมกับ Cisco DirSync ก็ได้



รูปที่ 3.87 การเปิดใช้งาน Cisco Tftp

3.3.17. การตั้งค่าให้กับ Management และ Access Switch

โดยให้มีการใช้งาน VLAN 1 โดยกำหนดให้มี IP Address ตามที่กำหนดในตารางที่ 3.1 และทำการ Config ให้มีการใช้งาน RADIUS Server พร้อมทั้งสร้าง Local Admin สำหรับเข้าใช้งานในกรณีที่ RADIUS Server หยุดการทำงาน โดยใช้ชุดคำสั่งดังนี้

username ***** privilege 15 password 7 ******

aaa new-model

aaa authentication login default group radius local

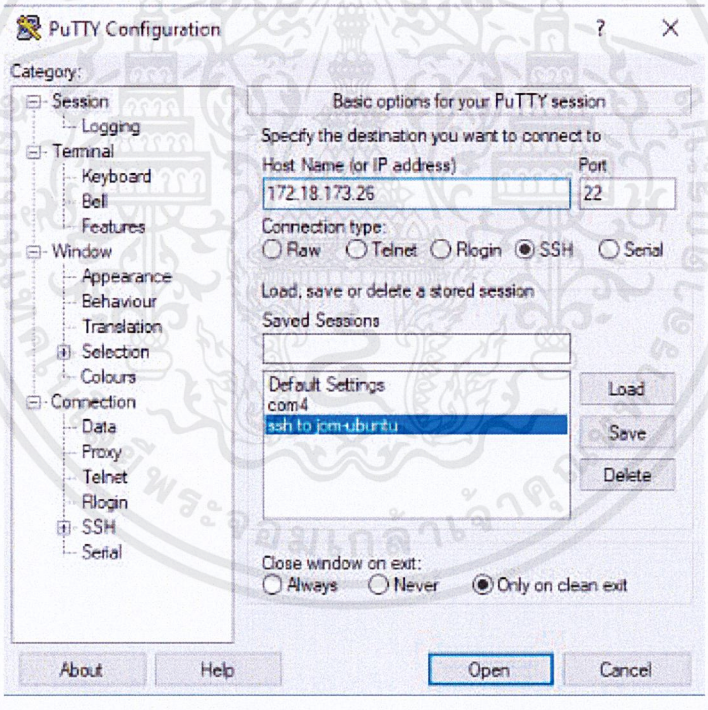
radius server jom 172.18.173.26 auth-port 1812 acct-port 1813 key *****

บทที่ 4
ผลการทดลอง

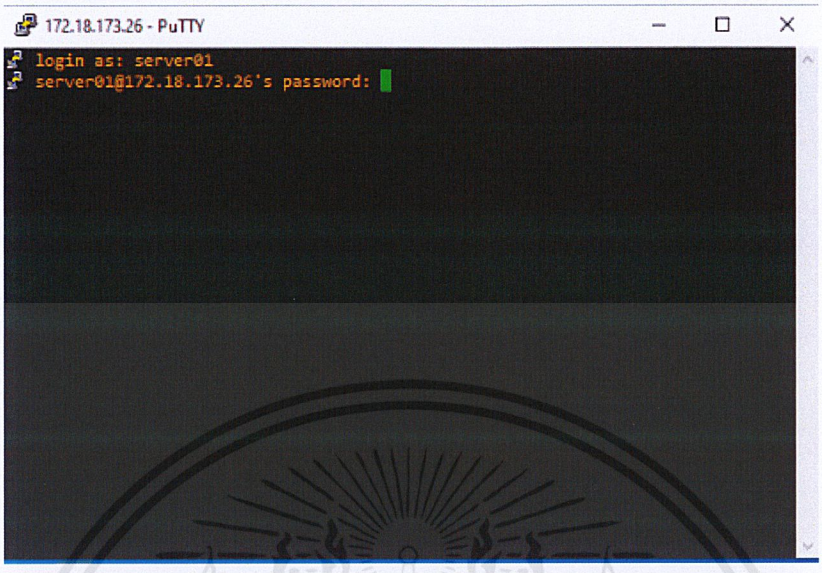
โดยหลังจากที่ได้ทำการติดตั้งระบบจำลองเสร็จเรียบร้อยก็ต้องทำการทดสอบการทำงานในส่วนต่างๆ ซึ่งมีการทดสอบดังต่อไปนี้

4.1 การเข้าใช้งานหน้า Console ของ Ubuntu 18.04 ผ่านทาง SSH

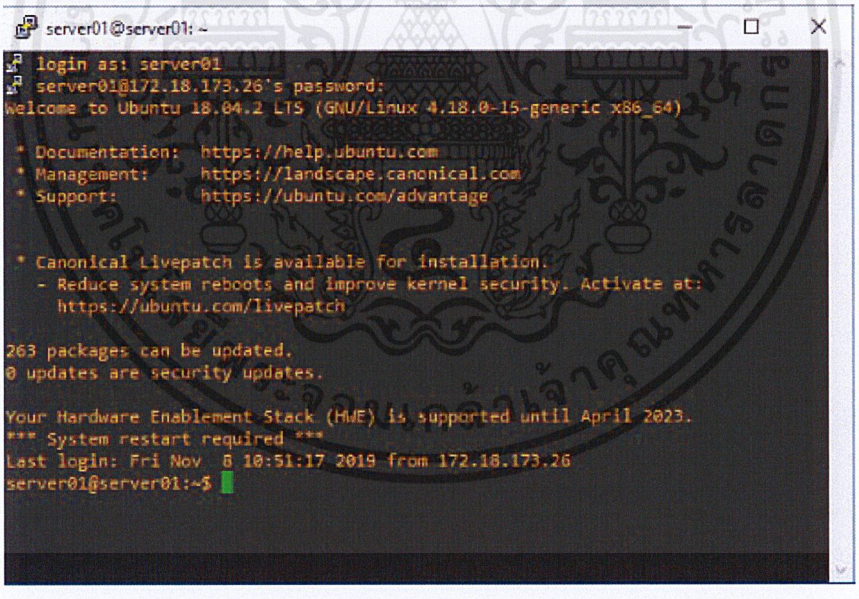
โดยทำการเชื่อมต่อเข้าใช้งานด้วยโปรแกรม putty โดยใช้ IP Address คือ 172.18.173.26 ของ Ubuntu



รูปที่ 4.1 การเชื่อมต่อ IP 172.18.173.26 ผ่านโปรโตคอล SSH



รูปที่ 4.2 การ Login เข้าใช้งานด้วย Hostname ของเครื่อง Ubuntu



รูปที่ 4.3 การเข้าใช้งานหน้า Console ของ Ubuntu

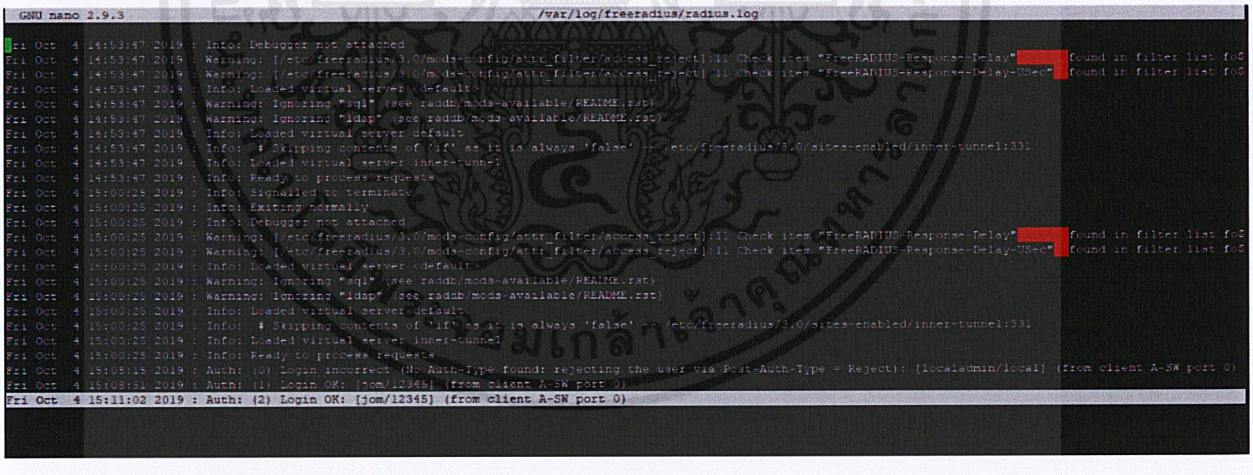
4.2 ทดสอบการเข้าไป Config อุปกรณ์

โดยทำการเข้าไป Config อุปกรณ์ในระบบเครือข่ายด้วยบัญชีผู้ใช้ที่ถูกสร้างไว้ภายใน RADIUS Server ซึ่งในที่นี้จะยกตัวอย่างการเข้าไปแก้ไขการตั้งค่าของ Access Switch ซึ่งมีผลดังนี้

- ทำการ Login เข้าไป Config โดยใช้ Users ที่สร้างไว้ภายใน RADIUS Server จะได้ผลดังรูปที่ 4.4

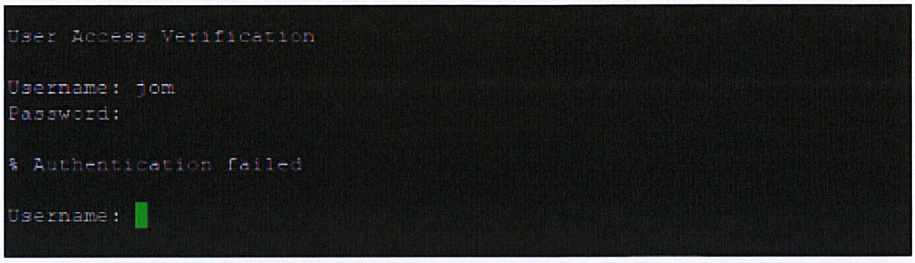
รูปที่ 4.4 การ Login เข้าใช้งานด้วยบัญชีผู้ใช้งานใน RADIUS Server

- สามารถเข้าไปตรวจสอบไฟล์log ได้ดังรูปที่ 4.5 ซึ่งจะสามารถระบุตัว Users และระบุได้ว่าเข้าไปจัดการ Config อุปกรณ์ตัวใดในระบบ



รูปที่ 4.5 Log แสดงการเข้าถึงของบัญชีผู้ใช้งานที่เข้ามา Config อุปกรณ์

- หากเกิดกรณีที่ RADIUS Server หยุดการทำงานจะไม่สามารถเข้าไปจัดการ Config อุปกรณ์โดยใช้ Usersที่สร้างไว้ใน RADIUS Server ได้ ดังรูปที่ 4.6



รูปที่ 4.6 การ Login ด้วยบัญชีผู้ใช้งานที่มีอยู่ใน RADIUS Server โดยที่ RADIUS Server หยุดการทำงาน

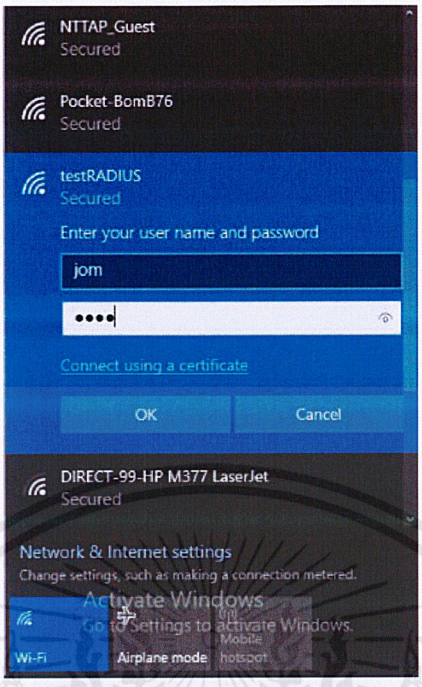
- โดยในกรณีที่ RADIUS Server หยุดการทำงานแล้วต้องการเข้าไป Config อุปกรณ์ ก็สามารถใช้การ Login โดยใช้ Local Admin ที่ถูกสร้างไว้ในฐานข้อมูลของตัวอุปกรณ์ ดังรูปที่ 4.7

รูปที่ 4.7 การ Login ด้วยบัญชี Local Admin ของอุปกรณ์

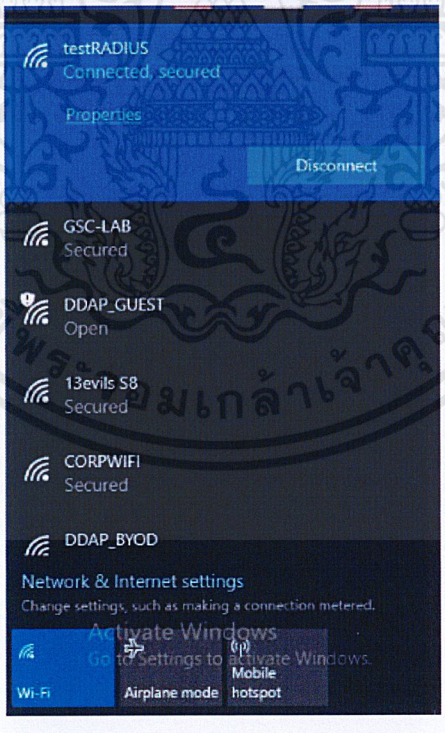
4.3 ทดสอบการเข้าใช้งานระบบเครือข่าย

โดยทำการเชื่อมต่อเข้าใช้งานด้วยบัญชีผู้ใช้ที่สร้างไว้ภายใน RADIUS Server ทั้งการเชื่อมต่อจากเครื่องคอมพิวเตอร์และจากโทรศัพท์มือถือ

- โดยในที่นี้จะทำการเชื่อมต่อกับ WLANs ที่ชื่อ testRADIUS และใช้บัญชีที่ถูกสร้างไว้ใน RADIUS Server ในการล็อกอิน ดังรูปที่ 4.8 และ 4.9

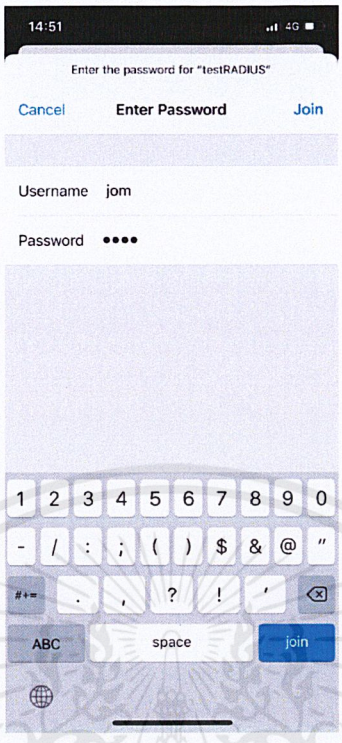


รูปที่ 4.8 การเชื่อมต่อเครือข่ายโดยใช้บัญชีผู้ใช้งานใน RADIUS Server (เชื่อมต่อจากคอมพิวเตอร์)



รูปที่ 4.9 การเชื่อมต่อเครือข่ายโดยสำเร็จ (เชื่อมต่อจากคอมพิวเตอร์)

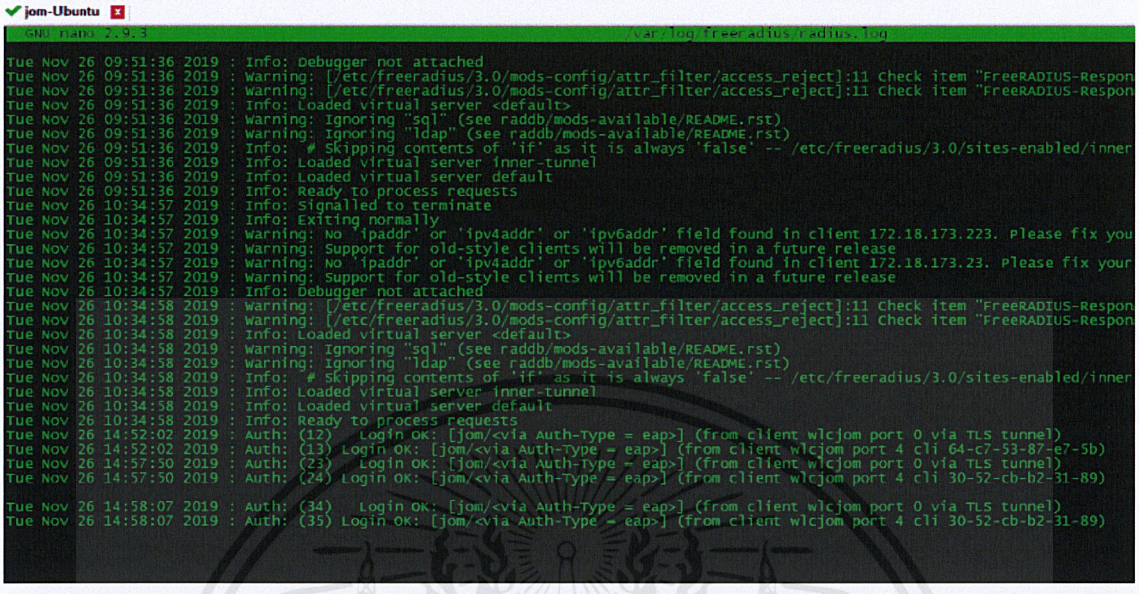
- ส่วนการเชื่อมต่อผ่านทางโทรศัพท์มือถือ จะเป็นไปดังรูปที่ 4.10 และ 4.11



รูปที่ 4.10 การเชื่อมต่อเครือข่ายโดยใช้บัญชีผู้ใช้งานใน RADIUS Server (เชื่อมต่อจากโทรศัพท์)

รูปที่ 4.11 การเชื่อมต่อเครือข่ายสำเร็จ (เชื่อมต่อจากโทรศัพท์)

- เมื่อทำการเข้าไปตรวจสอบดู log ภายใน RADIUS Server จะได้ผลดังรูปที่ 4.9

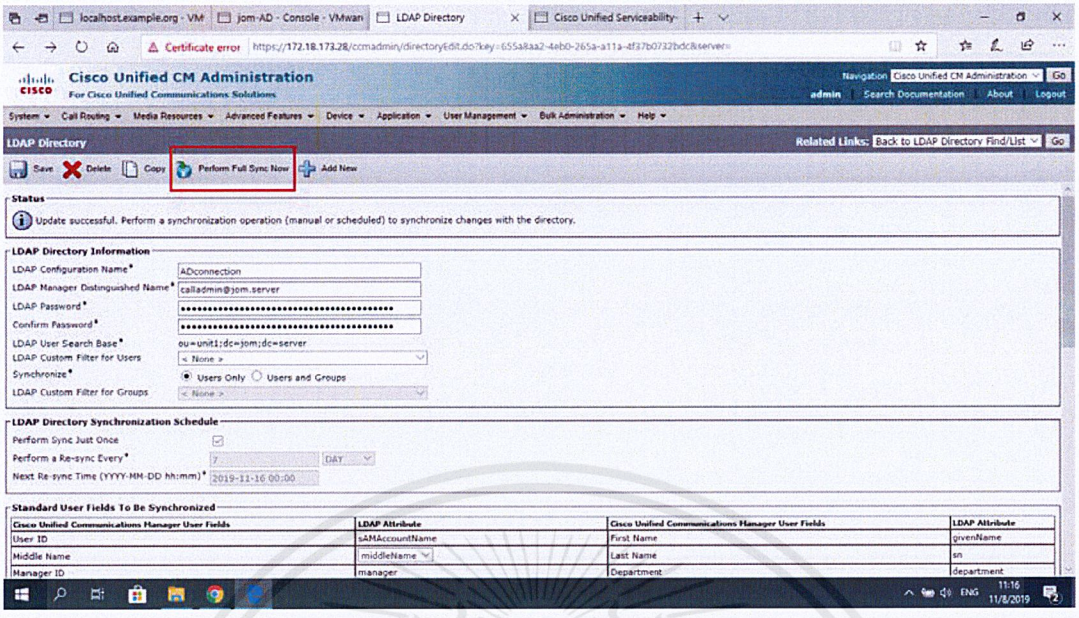


รูปที่ 4.12 การแสดงผล Log ภายใน RADIUS Server

4.4 ทดสอบการทำงานของ LDAP Directory

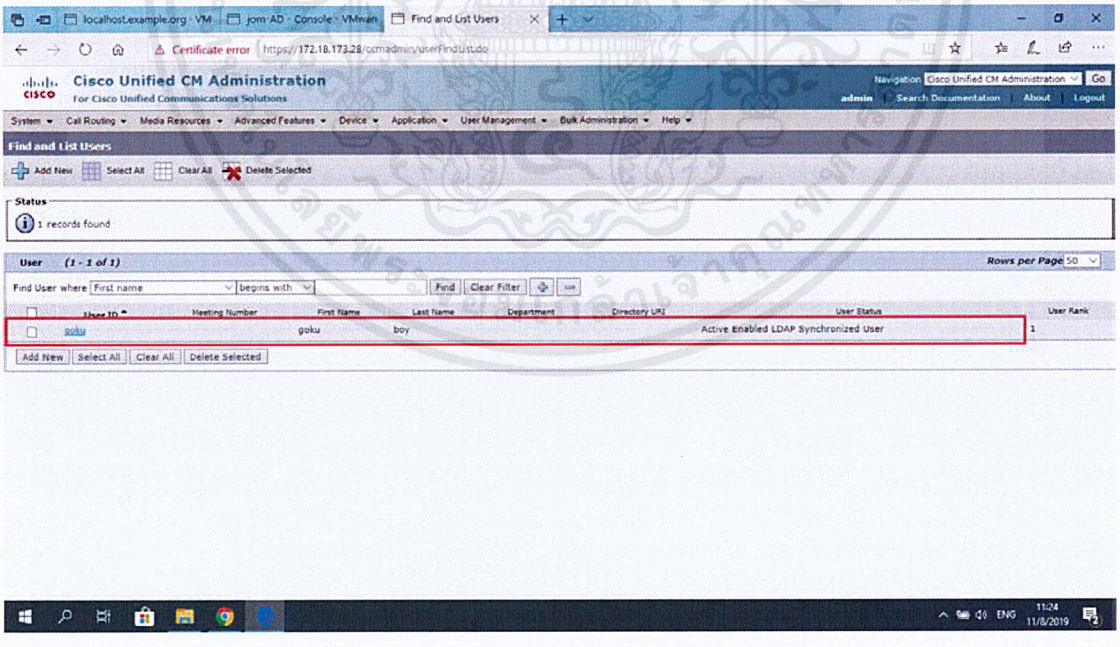
ทำการทดสอบ LDAP Directory ที่ถูกสร้างไว้ภายใน CUCM ที่สร้างไว้เพื่อให้ทำการดึงข้อมูลบัญชีผู้ใช้มาจาก Active Directory

- โดยทำการเข้าไปยัง LDAP Directory ที่ถูกสร้างไว้แล้วทำการกด perform full sync now ดังรูปที่ 4.13



รูปที่ 4.13 การทำการดึงข้อมูลจาก Active Directory

- จากนั้นทำการเข้าไปดูผลที่ User Management -> End Users ซึ่งจะสังเกต User Status ได้ว่าเป็น Active Enabled LDAP Synchronized User ดังรูปที่ 4.14 ซึ่งก็คือเป็น User ที่ถูกดึงมาจาก Active Directory ผ่านทาง LDAP นั่นเอง

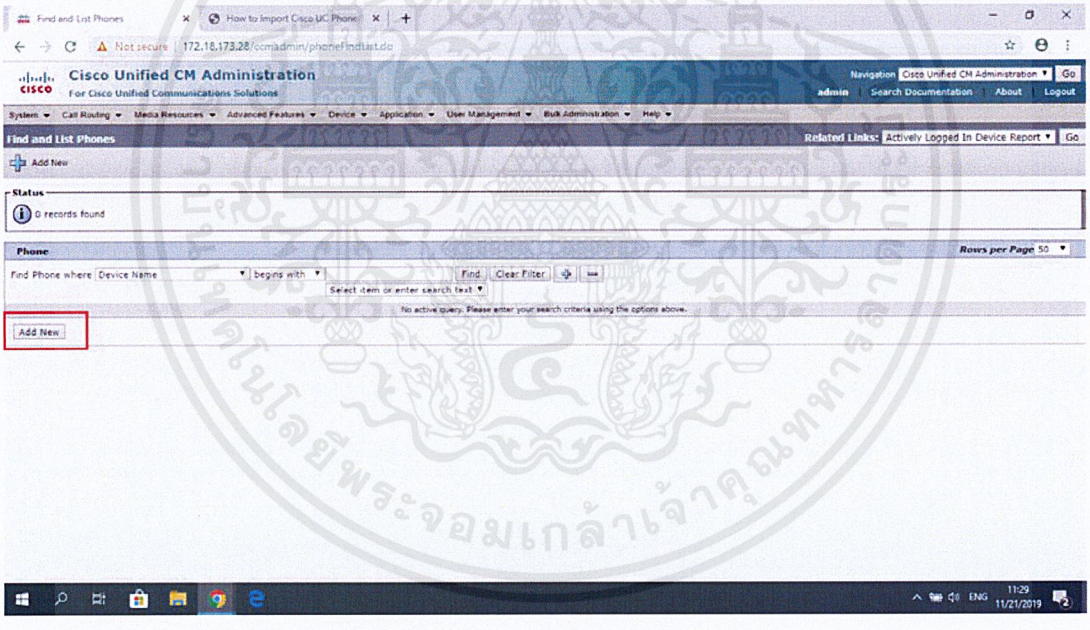


รูปที่ 4.14 รายชื่อบัญชีผู้ใช้งานที่ถูกเพิ่มเข้ามาจาก Active Directory

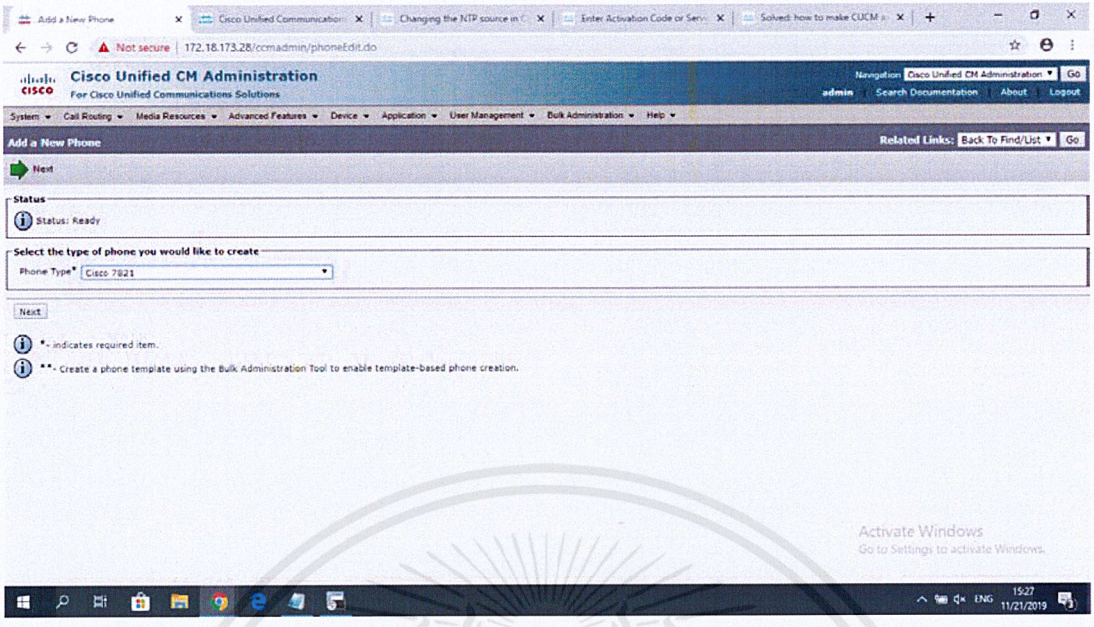
4.5 ทดสอบการทำงานของ CUCM

โดยทำการทดสอบว่าสามารถใช้งานจัดการการสื่อสารด้วยโทรศัพท์ IP Phone ได้จริง

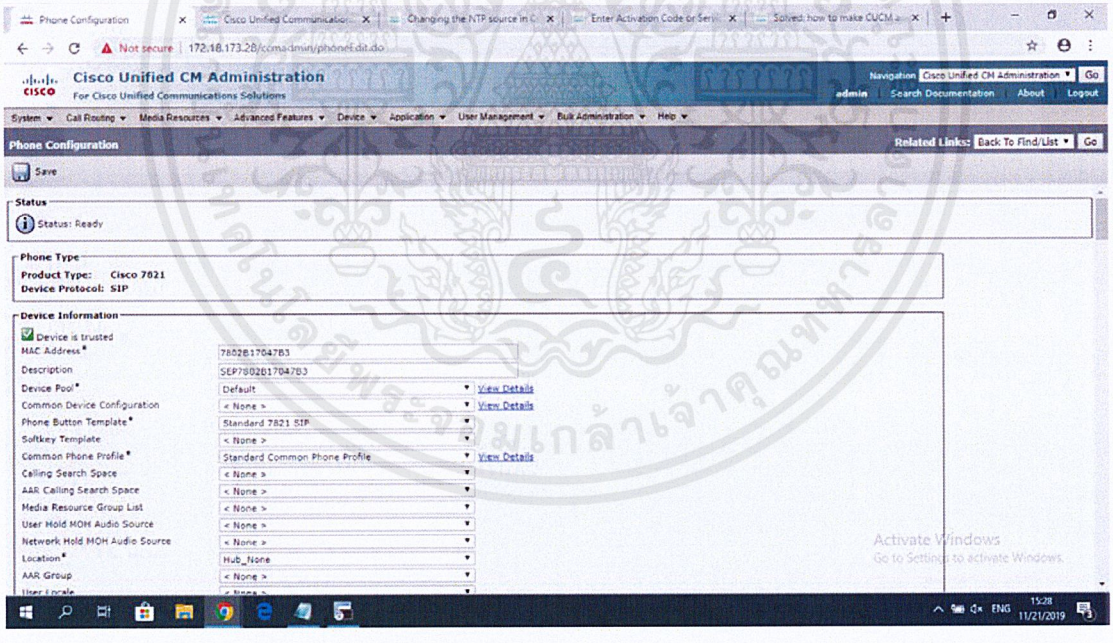
- การทดสอบเพิ่มโทรศัพท์เข้าไปในระบบ ซึ่งมีขั้นตอนดังนี้
    1. เข้าไปยัง Devices -> Phones แล้วทำการ Add new ดังรูปที่ 4.15
    2. ทำการเลือกรุ่นของโทรศัพท์ที่ต้องการจะเพิ่มเข้ามาในระบบ โดยในที่นี้ใช้โทรศัพท์ Cisco IP Phone 7821 ดังรูปที่ 4.16
    3. จากนั้นจะเป็นตั้งค่าให้กับโทรศัพท์ที่เพิ่มเข้ามา ดังรูปที่ 4.17 ซึ่งใช้ในที่นี้ให้ทำการกำหนด User ที่เป็นเจ้าของโทรศัพท์แต่ละเครื่องด้วย ดังรูปที่ 4.18
    1. เมื่อเสร็จสิ้นการเพิ่มโทรศัพท์เข้ามาในระบบจะสามารถเข้าไปตรวจสอบได้โดยเข้าไปที่ Devices -> Phones แล้วทำการกด Find ได้ผลดังรูปที่ 4.19



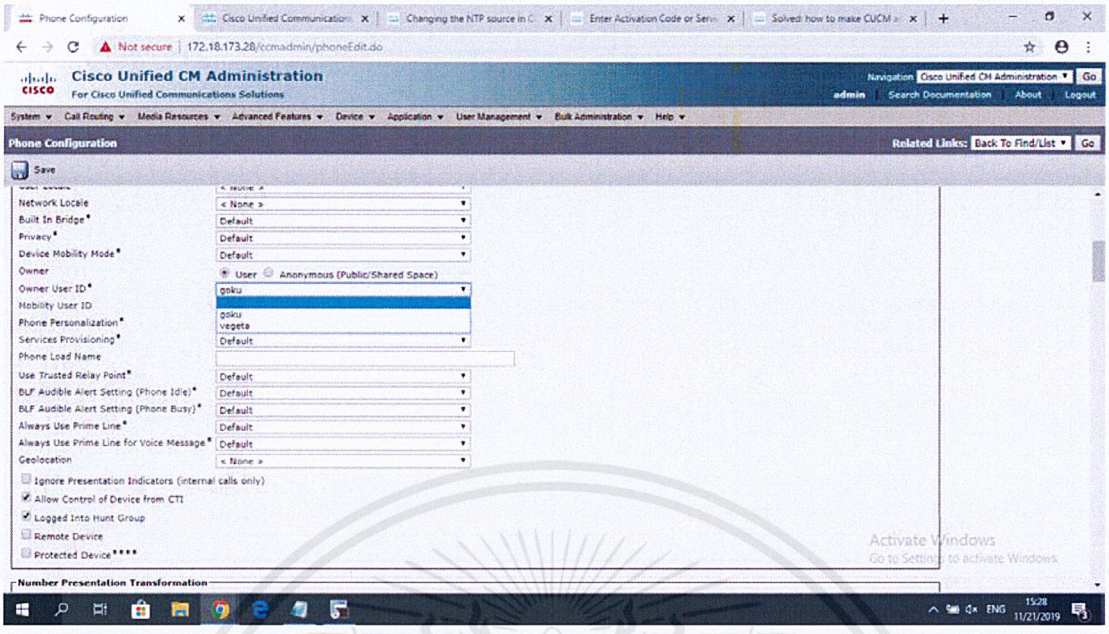
รูปที่ 4.15 การเพิ่มโทรศัพท์เข้าสู่ CUCM



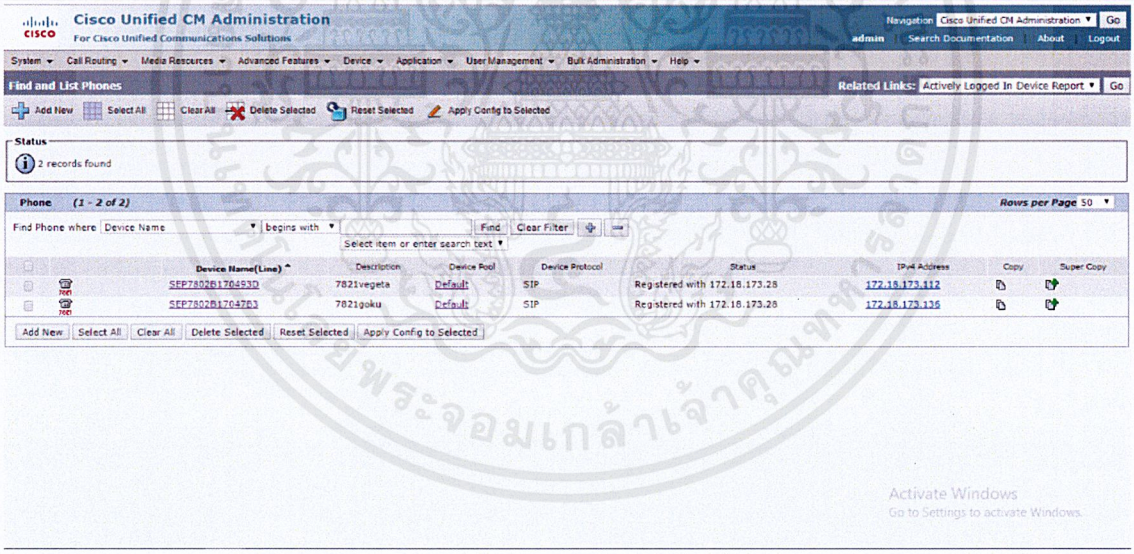
รูปที่ 4.16 การเลือกรุ่นของโทรศัพท์ที่ต้องการ



รูปที่ 4.17 การตั้งค่าให้กับโทรศัพท์ 1

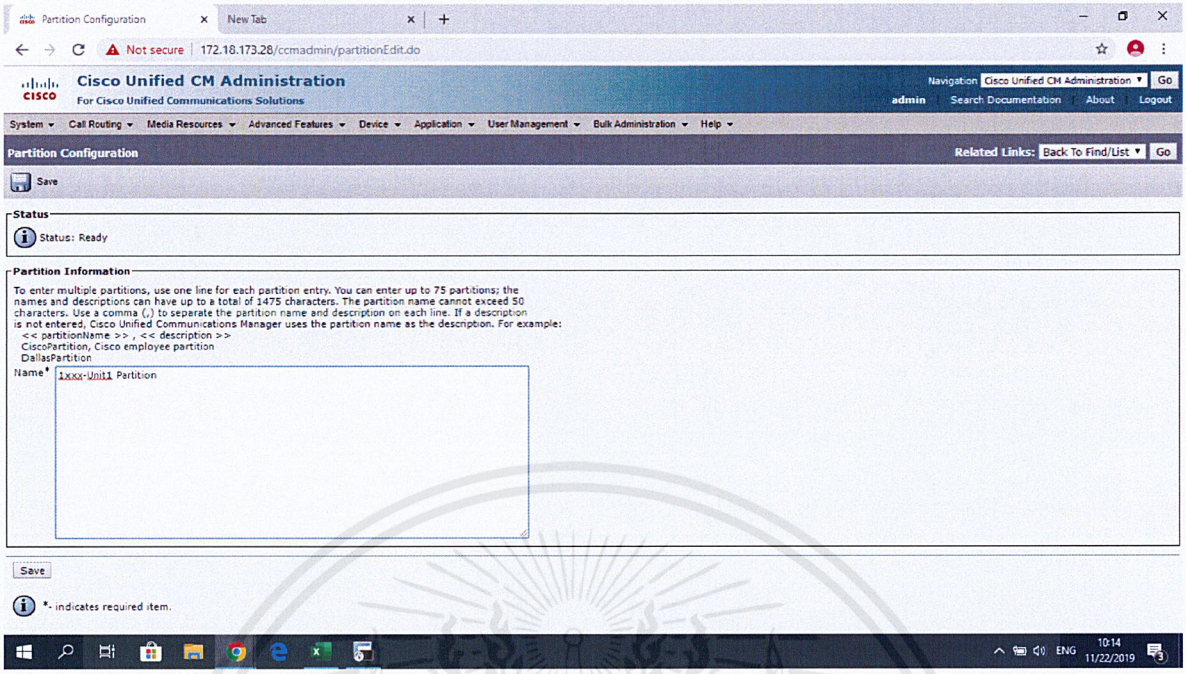


รูปที่ 4.18 การตั้งค่าให้กับโทรศัพท์ 2

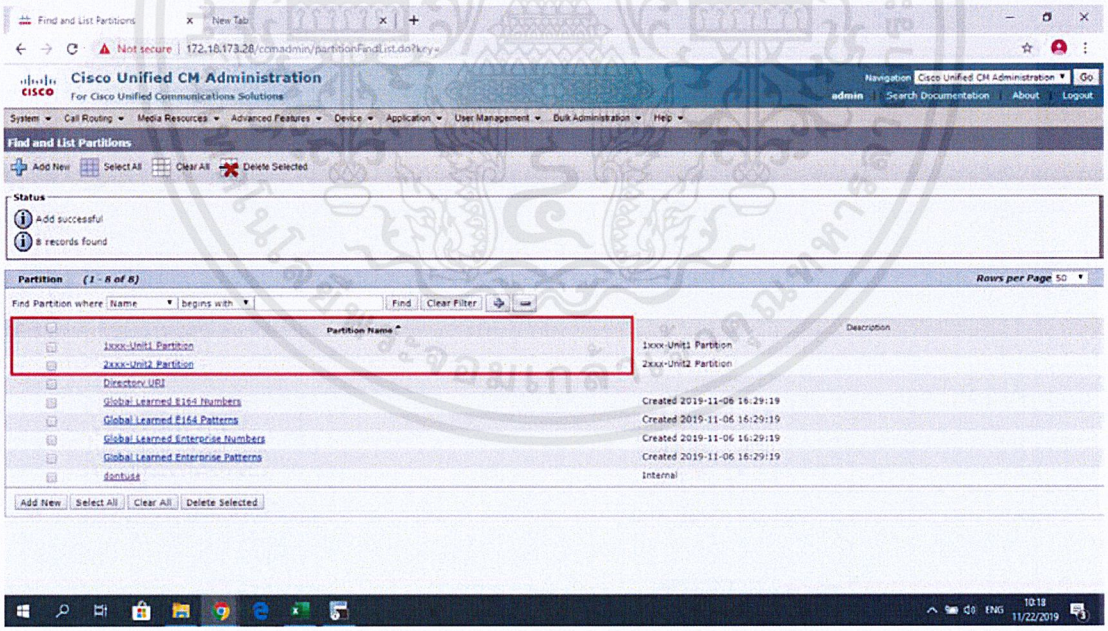


รูปที่ 4.19 รายชื่อโทรศัพท์ที่ถูกเพิ่มเข้ามาใน CUCM

- การทดสอบสร้าง Partition สำหรับจำแนกรูปแบบของหมายเลขโทรศัพท์ โดยเข้าไปที่ Call Routing -> Class of Control -> Partition แล้วทำการ Add new โดยใช้ชื่อว่า 1xxx-Unit1 Partition และ 2xxx-Unit2 Partition ดังรูปที่ 4.20 และ 4.21

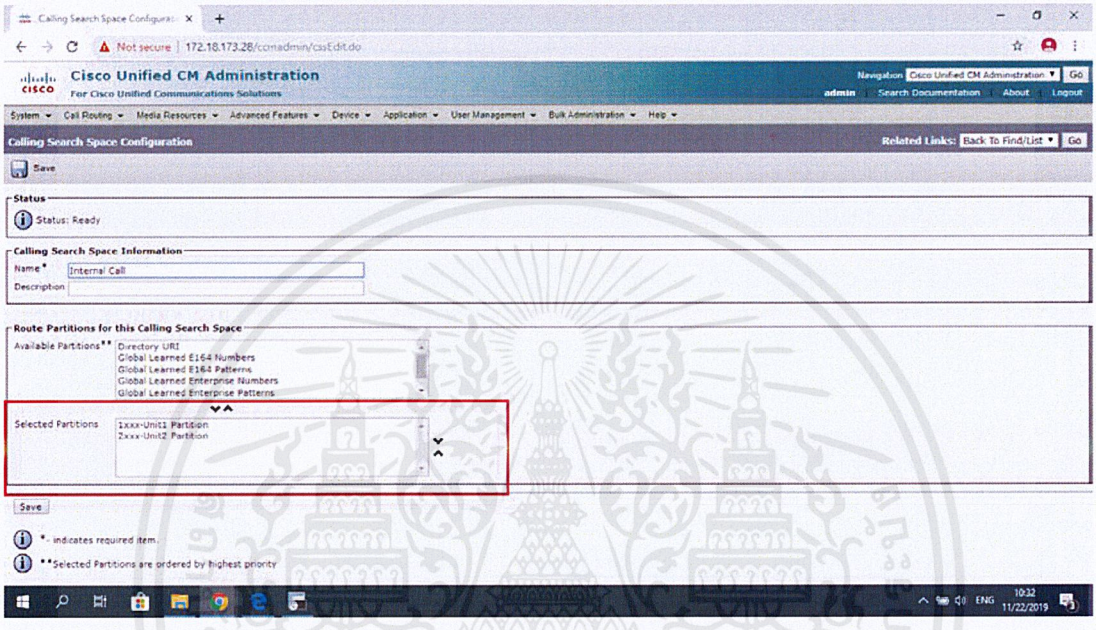


รูปที่ 4.20 การสร้าง Partition



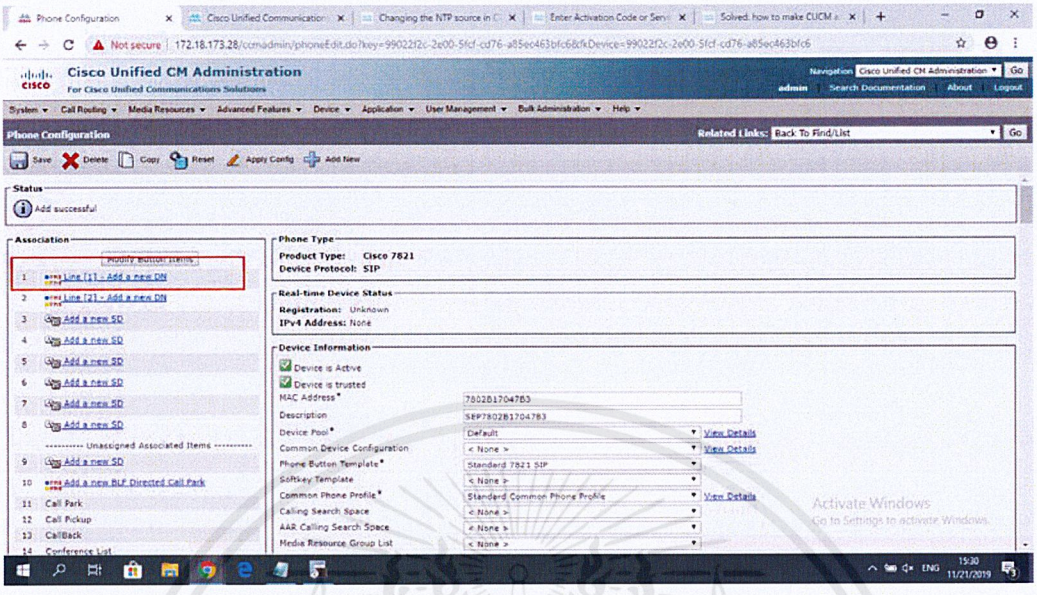
รูปที่ 4.21 รายชื่อ Partition ที่ถูกสร้างไว้

- การทดสอบสร้าง Calling Search Space(CSS) สำหรับรวบรวมรูปแบบของหมายเลขโทรศัพท์ที่สามารถติดต่อหากันได้ โดยเข้าไปที่ Call Routing -> Class of Control -> Calling Search Space แล้วทำการ Add new โดยตั้งชื่อว่า Internal Call และเพิ่ม Partitionที่สร้างไว้เข้าไป ดังรูปที่ 4.22

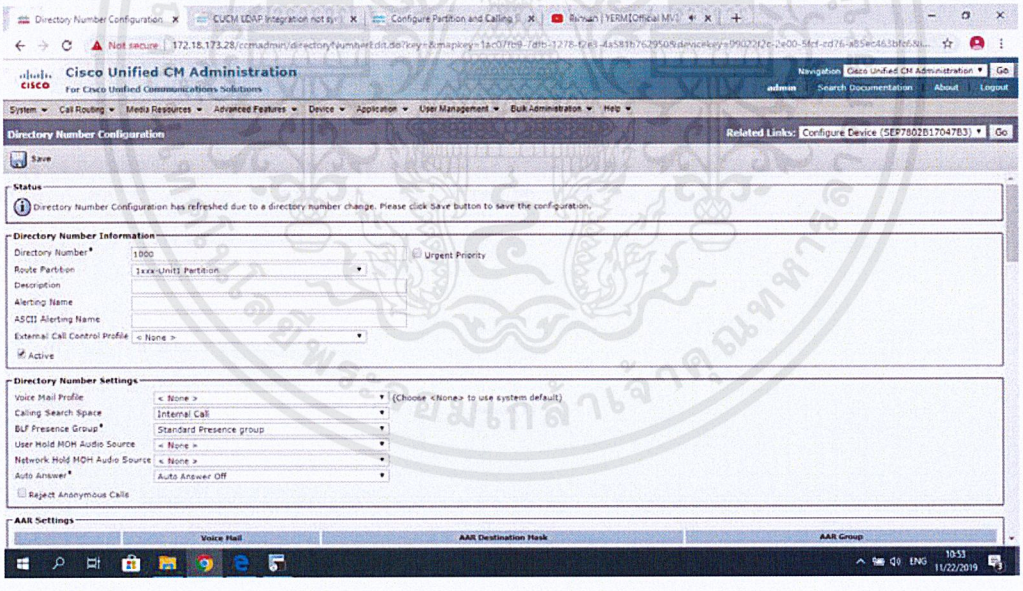


รูปที่ 4.22 การสร้าง CSS และการเพิ่ม Partition เข้าสู่ CSS

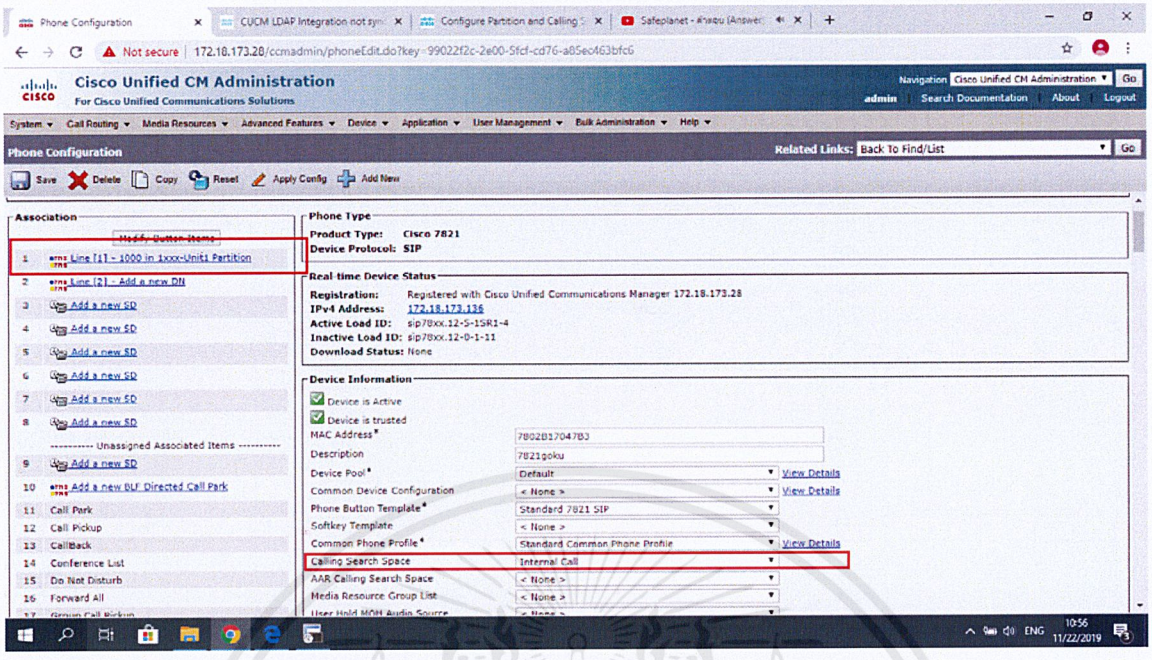
- ในส่วนของการทดสอบการโทรจริง จะสามารถใช้โทรได้จริงก็ต่อเมื่อมีการเพิ่มหมายเลขโทรศัพท์ให้กับโทรศัพท์ในระบบแต่ละเครื่อง พร้อมทั้งกำหนด Partition และ CSS ที่ใช้สำหรับการ Call Routing ซึ่งสามารถทำได้ดังรูปที่ 4.23, 4.24 และ 4.25 ตามลำดับ
- โดยกำหนดหมายเลขโทรศัพท์สำหรับใช้ในการทดสอบดังตารางที่ 4.1



รูปที่ 4.23 การเพิ่มหมายเลขโทรศัพท์ 1



รูปที่ 4.24 การเพิ่มหมายเลขโทรศัพท์ 2



รูปที่ 4.25 การเพิ่ม Partition และ CSS ให้กับโทรศัพท์

ตารางที่ 4.1 ข้อมูลและหมายเลขโทรศัพท์สำหรับใช้ในการทดสอบ

โทรศัพท์	IP Address	หมายเลขโทรศัพท์
7821vegeta	172.18.173.112	2000
7821goku	172.18.173.136	1000

- มีผลการทดลองโทรผ่านระบบเครือข่าย ดังนี้

1. หากมีการเพิ่ม CSS กลุ่มเดียวกันให้กับโทรศัพท์ทั้งสองเครื่อง เมื่อทำการโทรหากันจะสามารถติดต่อกันได้ เนื่องจากมีการค้นหาหมายเลขโดยใช้รูปแบบเดียวกัน (CSS กลุ่มเดียวกัน)
2. หากมีการเพิ่ม CSS ให้เพียงหมายเลข 1000 ก็จะยังสามารถโทรหาอีกหมายเลข 2000 ได้ถ้าหากภายใน CSS ที่ทำการเพิ่มให้หมายเลขนั้น มี Partition ของอีกหมายเลขอยู่ด้วย แต่หากไม่มีก็จะไม่สามารถติดต่อกันได้ เนื่องจากใน CSS ที่ทำการเพิ่มไปนั้นมีการค้นหาหมายเลขใน Partition อื่นด้วย

3. หากไม่มีการเพิ่ม CSS ให้ทั้งสองหมายเลข ทั้งสองหมายเลขก็จะไม่สามารถติดต่อหากันได้ เนื่องจากอยู่คนละ Partition กัน เนื่องจากเป็นรูปแบบหมายเลขโทรศัพท์ที่แตกต่างกัน
4. หากไม่มีการเพิ่ม CSS ให้ทั้งสองหมายเลข แต่กำหนดให้ทั้งสองหมายเลขอยู่ในPartition เดียวกัน จะสามารถโทรหากันได้เนื่องจากจะถือว่าถูกจัดอยู่ในรูปแบบหมายเลขโทรศัพท์แบบเดียวกัน

จากการทดสอบการทำงานของระบบโทรศัพท์ดังที่กล่าวมานั้น จะสามารถสรุปได้ว่าระบบการจัดการ(CUCM) ที่ทำการติดตั้งไปสามารถใช้งานได้จริงและมีการทำงานที่สมบูรณ์ไม่ผิดพลาด

บทที่ 5
สรุปผลการดำเนินงาน

ในการดำเนินการจัดทำโครงงานนั้นได้มีการออกแบบระบบเครือข่ายให้ตรงตามความต้องการของลูกค้ามากที่สุด โดยทางลูกค้ามีความต้องใช้งานให้ระบบเครือข่ายสามารถยืนยันตัวตนและจำกัดสิทธิ์ในการเข้าใช้งาน และต้องการติดตั้งระบบการสื่อสารภายในองค์กร โดยให้คำนึงถึงความปลอดภัยในการนำไปใช้งาน ความสะดวกในการบริหารจัดการ และการใช้ต้นทุนที่มีให้เกิดความคุ้มค่ามากที่สุด

โดยหลังการติดตั้ง และทดสอบระบบเครือข่ายจำลองภายในแลปของทางบริษัทเพื่อจัดทำเป็น POC ในการนำเสนอลูกค้านั้น สามารถนำไปใช้เพื่ออำนวยความสะดวกในการทดสอบการทำงานต่างๆและใช้สร้างความเชื่อมั่นให้กับลูกค้าว่าระบบนั้นสามารถใช้งานได้จริง โดยได้มีการเปิดให้ทางลูกค้าเข้ามาทำการทดสอบการทำงานของระบบ ซึ่งทางลูกค้าได้มีการยืนยันว่าระบบที่นำเสนอไปนั้นสามารถทำงานได้ตรงตามความต้องการ ทำให้ทางลูกค้าเกิดความพึงพอใจและพร้อมทำการจัดซื้อระบบเครือข่ายเพื่อนำไปติดตั้งในพื้นที่จริงในอนาคต

เอกสารอ้างอิง

[1] Cisco System, **The Hierarchical Network Design Model.** ที่มา: https://www.cisco.com/web/learning/netacad/demos/CCNP1v30/ch1/1_1_1/index.html

[2] NTP server. ที่มา: https://saixiii.com/what-is-ntp/

[3] freeRADIUS, **FreeRADIUS Documentation.** ที่มา: https://networkradius.com/doc/3.0.10/concepts/introduction/AAA.html

[4] Cisco System, **Configure Partition and Calling Search Space** ที่มา: https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-callmanager/22325-part-css-tn.html

[5] Cisco System, **Cisco UCS C220 M3 Datasheet.** ที่มา: https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m3-sff-specsheet.pdf

[6] Cisco System, **Cisco Catalyst 2960-L Series Switch Datasheet.** ที่มา: https://www.cisco.com/c/dam/global/th_th/assets/pdfs/cisco_catalyst_2960-l_series_switches_data_sheet_v5_th.pdf

[7] Cisco System, **Software Configuration Guide, Cisco IOS Release 15.2(5)E (Catalyst 2960-L Switches)** ที่มา: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960l/software/15-2_5_e/config-guide/b_1525e_consolidated_2960l_cg/b_1525e_consolidated_2960l_cg_chapter_0100011.html

[8] Cisco System, **RADIUS Server Authentication of Management Users on Wireless LAN Controller (WLC) Configuration Example** ที่มา: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71989-manage-wlc-users-radius.html